►**B**

BESCHLUSS DES RATES

vom 19. März 2001

über die Annahme der Sicherheitsvorschriften des Rates

(2001/264/EG)

(ABl. L 101 vom 11.4.2001, S. 1)

Geändert durch:

		Amtsblatt		
		Nr.	Seite	Datum
►**M1**	Beschluss 2004/194/EG des Rates vom 10. Februar 2004	L 63	48	28.2.2004

▼B

BESCHLUSS DES RATES

vom 19. März 2001

über die Annahme der Sicherheitsvorschriften des Rates

(2001/264/EG)

DER RAT DER EUROPÄISCHEN UNION —

gestützt auf den Vertrag zur Gründung der Europäischen Gemeinschaft, insbesondere auf Artikel 207 Absatz 3,

gestützt auf den Beschluss 2000/396/EG, EGKS, Euratom des Rates vom 5. Juni 2000 zur Festlegung seiner Geschäftsordnung [1], insbesondere auf Artikel 24,

in Erwägung nachstehender Gründe:

(1) Für die Ausweitung der Tätigkeiten des Rates in Bereichen, die ein bestimmtes Maß an Geheimhaltung erfordern, sollte ein umfassendes Sicherheitssystem geschaffen werden, das den Rat, sein Generalsekretariat und die Mitgliedstaaten einbezieht.

(2) Im Rahmen eines derartigen Systems sollten alle in diesem Bereich durch frühere Beschlüsse und Bestimmungen behandelten Themen in einem einzigen Text zusammengefasst werden.

(3) In der Praxis werden die meisten EU-Verschlusssachen, die als „CONFIDENTIEL UE“ oder höher eingestuft werden, die Gemeinsame Sicherheits- und Verteidigungspolitik betreffen.

(4) Um die Effizienz des so geschaffenen Sicherheitssystems zu gewährleisten, sollten die Mitgliedstaaten in der Weise daran beteiligt werden, dass sie einzelstaatliche Maßnahmen treffen, mit denen die Einhaltung der Bestimmungen dieses Beschlusses in den Fällen garantiert wird, in denen zuständige Behörden und Bedienstete der Mitgliedstaaten mit EU-Verschlusssachen zu tun haben.

(5) Der Rat begrüßt die Absicht der Kommission, bis zum Zeitpunkt der Anwendung dieses Beschlusses ein mit den Anhängen im Einklang stehendes umfassendes System zu schaffen, durch das ein reibungsloser Ablauf des Beschlussfassungsprozesses in der Union sichergestellt wird.

(6) Der Rat weist darauf hin, dass es wichtig ist, gegebenenfalls das Europäische Parlament und die Kommission an den Geheimhaltungsregeln und -normen, die zum Schutz der Interessen der Union und ihrer Mitgliedstaaten erforderlich sind, zu beteiligen.

(7) Dieser Beschluss lässt Artikel 255 des Vertrags und die zu seiner Durchführung erlassenen Rechtsakte unberührt.

(8) Dieser Beschluss berührt nicht die derzeitigen Verfahren der Mitgliedstaaten zur Unterrichtung ihrer jeweiligen Parlamente über die Tätigkeiten der Union —

BESCHLIESST:

Artikel 1

Die im Anhang enthaltenen Sicherheitsvorschriften des Rates werden angenommen.

Artikel 2

(1) Der Generalsekretär/Hohe Vertreter trifft geeignete Maßnahmen, um dafür zu sorgen, dass die Sicherheitsvorschriften nach Artikel 1 beim Umgang mit EU-Verschlusssachen im Generalsekretariat des Rates von dessen Beamten und sonstigen Bediensteten, von externen

[1] ABl. L 149 vom 23.6.2000, S. 21.

▼B

Vertragspartnern des Generalsekretariats des Rates und von an das Generalsekretariat des Rates abgeordnetem Personal eingehalten werden und ihre Einhaltung auch in Gebäuden des Rates und in dezentralen Einrichtungen der EU ([1]) gesichert ist.

(2) Die Mitgliedstaaten treffen im Einklang mit den einzelstaatlichen Regelungen geeignete Maßnahmen, um dafür zu sorgen, dass folgende Personengruppen beim Umgang mit EU-Verschlusssachen innerhalb ihrer Dienste und Gebäude die Sicherheitsvorschriften nach Artikel 1 einhalten:

a) die Mitglieder der Ständigen Vertretungen der Mitgliedstaaten bei der Europäischen Union sowie die Mitglieder der nationalen Delegationen, die an Tagungen des Rates oder seiner Gremien teilnehmen bzw. in sonstige Tätigkeiten des Rates einbezogen sind;

b) sonstige Mitglieder der nationalen Verwaltungen der Mitgliedstaaten, die mit EU-Verschlusssachen zu tun haben, unabhängig davon, ob sie im Hoheitsgebiet der Mitgliedstaaten oder außerhalb Dienst tun;

c) externe Vertragspartner der Mitgliedstaaten und von ihnen abgeordnetes Personal, die mit EU-Verschlusssachen zu tun haben.

Die Mitgliedstaaten unterrichten das Generalsekretariat des Rates unverzüglich über die getroffenen Maßnahmen.

(3) Die in den Absätzen 1 und 2 genannten Maßnahmen werden vor dem 30. November 2001 erlassen.

Artikel 3

Der Generalsekretär/Hohe Vertreter kann unter Beachtung der in Teil I des Anhangs enthaltenen Grundprinzipien und Mindeststandards für die Sicherheit Maßnahmen nach Teil II Abschnitt I Nummern 1 und 2 des Anhangs treffen.

Artikel 4

Der vorliegende Beschluss ersetzt ab dem Tage seiner Anwendung

a) den Beschluss 98/319/EG des Rates vom 27. April 1998 über das Verfahren zur Ermächtigung der Beamten und sonstigen Bediensteten des Generalsekretariats des Rates zum Zugang zu vom Rat verwahrten Verschlusssachen ([2]);

b) den Beschluss des Generalsekretärs/Hohen Vertreters vom 27. Juli 2000 über die im Generalsekretariat des Rates anzuwendenden Maßnahmen zum Schutz der als Verschlusssachen einzustufenden Informationen ([3]);

c) den Beschluss Nr. 433/97 des Generalsekretärs des Rates vom 22. Mai 1997 über die Sicherheitsüberprüfung der mit dem Betrieb des Cortesy-Systems beauftragten Beamten.

Artikel 5

(1) Dieser Beschluss wird am Tag seiner Veröffentlichung wirksam.

(2) Er gilt ab dem 1. Dezember 2001.

([1]) Siehe Schlussfolgerungen des Rates vom 10. November 2000.
([2]) ABl. L 140 vom 12.5.1998, S. 12.
([3]) ABl. C 239 vom 23.8.2000, S. 1.

▼B

ANHANG

SICHERHEITSVORSCHRIFTEN DES RATES DER EUROPÄISCHEN UNION

▼B

INHALT

▼B

TEIL I

GRUNDPRINZIPIEN UND MINDESTSTANDARDS FÜR DIE SICHERHEIT

EINLEITUNG

1. Die vorliegenden Bestimmungen enthalten die Grundprinzipien und Mindeststandards für die Sicherheit, die vom Rat, dem Generalsekretariat des Rates, den Mitgliedstaaten und den dezentralen Einrichtungen der Europäischen Union (nachstehend „dezentrale EU-Einrichtungen“ genannt) in angemessener Weise einzuhalten sind, damit die Sicherheit gewährleistet ist und darauf vertraut werden kann, dass ein gemeinsamer Sicherheitsstandard herrscht.

2. Unter „EU-Verschlusssachen“ sind alle Informationen und Materialien zu verstehen, deren unerlaubte Weitergabe den Interessen der EU oder eines oder mehrerer ihrer Mitgliedstaaten in unterschiedlichem Maße Schaden zufügen könnte, unabhängig davon, ob es sich um ursprüngliche EU-Verschlusssachen handelt oder um Verschlusssachen, die von Mitgliedstaaten, Drittländern oder internationalen Organisationen stammen.

3. Im gesamten Text dieser Sicherheitsvorschriften bedeutet

   a) „Dokument“ jede Form von Schreiben, Aufzeichnung, Protokoll, Bericht, Memorandum, Signal/Botschaft, Skizze, Photo, Dia, Film, Karte, Schaubild, Plan, Notizbuch, Matrize, Kohlepapier, Schreibmaschinen- oder Druckerfarbband, Magnetband, Kassette, Computer-Diskette, CD-ROM oder anderer materieller Träger, auf denen Informationen gespeichert sind;

   b) „Material“ dasselbe wie „Dokument“ gemäß der Definition unter Buchstabe a) sowie jeden Ausrüstungsgegenstand und jede Waffe, die bereits hergestellt oder noch in der Herstellung befindlich sind.

4. Die Hauptziele im Bereich der Sicherheit sind:

   a) Schutz von EU-Verschlusssachen vor Spionage, Kenntnisnahme durch Unbefugte oder unerlaubter Weitergabe;

   b) Schutz von EU-Informationen, die in Kommunikations- und Informationssystemen und -netzen behandelt werden, vor Gefahren für ihre Integrität und Verfügbarkeit;

   c) Schutz von Einrichtungen, in denen EU-Informationen aufbewahrt werden, vor Sabotage und vorsätzlicher Beschädigung;

   d) im Falle eines Versagens der Sicherheitsvorkehrungen Bewertung des entstandenen Schadens, Begrenzung seiner Folgen und Durchführung der erforderlichen Maßnahmen zu seiner Behebung.

5. Die Grundlagen für die Schaffung einer soliden Sicherheitslage sind

   a) in jedem Mitgliedstaat eine nationale Sicherheitsorganisation, die dafür zuständig ist,

      i) Erkenntnisse über Spionage, Sabotage, Terrorismus und andere subversive Tätigkeiten zu sammeln und zu speichern sowie

      ii) ihre jeweilige Regierung und — über sie — den Rat über Art und Umfang von Bedrohungen der Sicherheit und entsprechende Schutzmaßnahmen zu informieren und zu beraten;

   b) in jedem Mitgliedstaat und im Generalsekretariat des Rates eine technische INFOSEC-Stelle, die dafür zuständig ist, in Zusammenarbeit mit der betreffenden Sicherheitsbehörde Informationen und Beratung über technische Bedrohungen der Sicherheit und entsprechende Schutzmaßnahmen zu liefern;

   c) eine regelmäßige Zusammenarbeit von Regierungsstellen, Einrichtungen und entsprechenden Dienststellen des Generalsekretariats des Rates, um erforderlichenfalls

      i) die schutzbedürftigen Informationen, Ressourcen und Einrichtungen und

      ii) gemeinsame Schutzstandards

      zu bestimmen und entsprechende Empfehlungen abzugeben.

6. Im Bereich der Geheimhaltung muss bei der Auswahl der schutzbedürftigen Informationen und Materialien und bei der Bewertung des Ausmaßes des erforderlichen Schutzes mit Sorgfalt vorgegangen und auf Erfahrungen zurückgegriffen werden. Es ist von entscheidender Bedeutung, dass das Ausmaß des Schutzes der Sicherheitsrelevanz der zu schützenden Informationen und Materialien entspricht. Im Interesse eines reibungslosen

▼B

Informationsflusses muss dafür gesorgt werden, dass eine zu hohe Einstufung von Verschlusssachen vermieden wird. Das Einstufungssystem ist das Instrument, mit dem diesen Grundsätzen Wirkung verliehen wird; ein entsprechendes Einstufungssystem sollte bei der Planung und Organisierung von Maßnahmen zur Bekämpfung von Spionage, Sabotage, Terrorismus und anderen Arten der Bedrohung angewandt werden, so dass die wichtigsten Gebäude, in denen Verschlusssachen aufbewahrt werden, und die sensibelsten Punkte innerhalb dieser Gebäude auch den größten Schutz erhalten.

GRUNDPRINZIPIEN

7. **Die Sicherheitsmaßnahmen sollen**

a) alle Personen, die Zugang zu Verschlusssachen haben, die Träger von Verschlusssachen und alle Gebäude, in denen sich derartige Verschlusssachen und wichtige Einrichtungen befinden, umfassen;

b) so ausgelegt sein, dass Personen, die aufgrund ihrer Stellung die Sicherheit von Verschlusssachen und wichtigen Einrichtungen, in denen Verschlusssachen aufbewahrt werden, gefährden könnten, erkannt und vom Zugang ausgeschlossen oder fern gehalten werden;

c) verhindern, dass unbefugte Personen Zugang zu Verschlusssachen oder zu Einrichtungen, in denen Verschlusssachen aufbewahrt werden, erhalten;

d) dafür sorgen, dass Verschlusssachen nur unter Beachtung des für alle Aspekte der Sicherheit grundlegenden Prinzips „Kenntnis nur wenn nötig“ verbreitet werden;

e) die Integrität (d. h. Verhinderung von Verfälschungen, unbefugten Änderungen oder unbefugten Löschungen) und die Verfügbarkeit (d. h. keine Verweigerung des Zugangs für Personen, die ihn benötigen und dazu befugt sind) aller Informationen, ob sie als Verschlusssachen eingestuft sind oder nicht, und insbesondere der in elektromagnetischer Form gespeicherten, verarbeiteten oder übermittelten Informationen, gewährleisten.

ORGANISATION DER SICHERHEIT

Gemeinsame Mindeststandards

8. Der Rat und jeder Mitgliedstaat sorgen dafür, dass gemeinsame Mindeststandards für die Sicherheit von allen Verwaltungs- und/oder Regierungsstellen, anderen EU-Organen und EU-Einrichtungen sowie den Vertragspartnern der EU eingehalten werden, so dass bei der Weitergabe von EU-Verschlusssachen darauf vertraut werden kann, dass diese mit derselben Sorgfalt behandelt werden. Zu diesen Mindeststandards gehören Kriterien für die Sicherheitsüberprüfung des Personals und Verfahren zum Schutz von EU-Verschlusssachen.

SICHERHEIT DES PERSONALS

Sicherheitsüberprüfung

9. Alle Personen, die Zugang zu Informationen erhalten wollen, die als „CONFIDENTIEL UE“ oder höher eingestuft sind, werden einer Sicherheitsüberprüfung unterzogen, bevor sie eine Zugangsermächtigung erhalten. Eine entsprechende Sicherheitsüberprüfung wird auch im Falle von Personen vorgenommen, zu deren Aufgaben der technische Betrieb oder die Wartung von Kommunikations- und Informationssystemen gehört, die Verschlusssachen enthalten. Bei der Sicherheitsüberprüfung soll festgestellt werden, ob die genannten Personen

a) von unzweifelhafter Loyalität sind;

b) hinsichtlich ihres Charakters und ihrer Diskretionsfähigkeit so beschaffen sind, dass ihre Integrität beim Umgang mit Verschlusssachen außer Zweifel steht;

c) eventuell aus dem Ausland oder von anderer Seite her leicht unter Druck gesetzt werden können, z. B. aufgrund ihres früheren Wohnsitzes oder früherer Verbindungen, die ein Sicherheitsrisiko darstellen könnten.

Besonders gründlich ist die Sicherheitsüberprüfung bei Personen vorzunehmen, die

d) Zugang zu Informationen des Geheimhaltungsgrades „TRÈS SECRET UE/EU TOP SECRET“ erhalten sollen;

e) Stellen bekleiden, bei denen sie regelmäßig mit einer beträchtlichen Menge an Informationen des Geheimhaltungsgrades „SECRET UE“ zu tun haben;

▼B

f) aufgrund ihres Aufgabenbereichs besonderen Zugang zu jeweils entscheidend wichtigen Kommunikations- oder Informationssystemen und somit Gelegenheit haben, sich unbefugt Zugang zu einer größeren Menge von EU-Verschlusssachen zu verschaffen oder in dem betreffenden Aufgabenbereich durch technische Sabotageakte schweren Schaden zu verursachen.

In den unter den Buchstaben d), e) und f) genannten Fällen soll soweit als nur möglich auf die Methode der Umfeldermittlung zurückgegriffen werden.

10. Werden Personen, für die die Notwendigkeit einer Kenntnis von Verschlusssachen nicht klar erwiesen ist, unter Umständen beschäftigt, unter denen sie Zugang zu EU-Verschlusssachen erhalten könnten (z. B. Boten, Sicherheitsbedienstete, Wartungs- und Reinigungspersonal usw.), so sind sie zuerst einer Sicherheitsüberprüfung zu unterziehen.

Verzeichnis der Zugangsermächtigungen

11. Alle Dienststellen, Gremien oder Einrichtungen, die mit EU-Verschlusssachen zu tun haben oder jeweils entscheidend wichtige Kommunikations- oder Informationssysteme verwalten, führen ein Verzeichnis der Zugangsermächtigungen des bei ihnen arbeitenden Personals. Jede Zugangsermächtigung ist erforderlichenfalls zu überprüfen, um sicherzustellen, dass sie der derzeitigen Tätigkeit der betreffenden Person entspricht; sie ist vorrangig zu überprüfen, wenn neue Informationen eingehen, denen zufolge eine weitere Beschäftigung dieser Person mit Verschlusssachen nicht länger mit den Sicherheitsinteressen vereinbar ist. Das Verzeichnis der Zugangsermächtigungen ist vom Geheimschutzbeauftragten der jeweiligen Dienststelle, des jeweiligen Gremiums beziehungsweise der jeweiligen Einrichtung zu führen.

Sicherheitsanweisungen für das Personal

12. Alle Angehörigen des Personals, die Stellen bekleiden, an denen sie Zugang zu Verschlusssachen erhalten könnten, sind bei Aufnahme ihrer Tätigkeit und danach in regelmäßigen Abständen eingehend über die Notwendigkeit von Sicherheitsbestimmungen und über die Verfahren zu ihrer Durchführung zu unterrichten. Es ist nützlich, von allen Angehörigen des Personals eine schriftliche Bestätigung zu verlangen, dass sie die für ihre Arbeit relevanten Sicherheitsbestimmungen in vollem Umfang verstehen.

Verantwortung der Führungskräfte

13. Führungskräfte haben die Pflicht, sich Kenntnis darüber zu verschaffen, welche ihrer Mitarbeiter mit Verschlusssachen zu tun haben oder über einen Zugang zu jeweils entscheidend wichtigen Kommunikations- oder Informationssystemen verfügen, sowie alle Vorfälle oder offensichtlichen Schwachpunkte von Personen, die sicherheitsrelevant sein könnten, festzuhalten und darüber zu berichten.

Sicherheitsstatus des Personals

14. Es sind Verfahren vorzusehen, um dafür zu sorgen, dass bei Bekanntwerden nachteiliger Informationen über eine Person festgestellt wird, ob diese Person mit Verschlusssachen zu tun hat oder über einen Zugang zu jeweils entscheidend wichtigen Kommunikations- oder Informationssystemen verfügt, und dass die betreffende Dienststelle hiervon unterrichtet wird. Ist klar erwiesen, dass die fragliche Person ein Sicherheitsrisiko darstellt, ist sie von Aufgaben, bei denen sie die Sicherheit gefährden könnte, auszuschließen oder fern zu halten.

MATERIELLER GEHEIMSCHUTZ

Schutzbedarf

15. Das Ausmaß der anzuwendenden Maßnahmen des materiellen Geheimschutzes zur Gewährleistung des Schutzes von EU-Verschlusssachen muss in angemessenem Verhältnis zum Geheimhaltungsgrad, zum Umfang und zur Bedrohung der entsprechenden Informationen und Materialien stehen. Es ist daher darauf zu achten, dass weder eine zu hohe noch eine zu niedrige Einstufung vorgenommen wird und dass die Einstufung regelmäßig überprüft wird. Alle Personen, die EU-Verschlusssachen verwahren, haben einheitliche Praktiken bei der Einstufung der Informationen anzuwenden und gemeinsame Schutzstandards für die Verwahrung, Übermittlung und Vernichtung schutzbedürftiger Informationen und Materialien zu beachten.

Kontrolle

16. Personen, die Bereiche, in denen sich ihnen anvertraute EU-Verschlusssachen befinden, unbeaufsichtigt lassen, müssen dafür sorgen, dass die Verschlusssachen sicher aufbewahrt und alle Sicherungsvorkehrungen

▼B

(Schlösser, Alarm usw.) aktiviert worden sind. Weitere hiervon unabhängige Kontrollen sind nach den Dienststunden durchzuführen.

Gebäudesicherheit

17. Gebäude, in denen sich EU-Verschlusssachen oder entscheidend wichtige Kommunikations- und Informationssysteme befinden, sind gegen unerlaubten Zutritt zu schützen. Die Art der Schutzmaßnahmen für EU-Verschlusssachen (z. B. Vergitterung von Fenstern, Schlösser an Türen, Wachen am Eingang, automatische Zugangskontrollsysteme, Sicherheitskontrollen und Rundgänge, Alarmsysteme, Einbruchmeldesysteme und Wachhunde) hängt von folgenden Faktoren ab:

    a) Geheimhaltungsgrad und Umfang der zu schützenden Informationen und Materialien sowie Ort ihrer Unterbringung im Gebäude;

    b) Qualität der Sicherheitsbehältnisse, in denen sich die Informationsträger und Materialien befinden, und

    c) Beschaffenheit und Lage des Gebäudes.

18. Die Art der Schutzmaßnahmen für Kommunikations- und Informationssysteme hängt in ähnlicher Weise von folgenden Faktoren ab: Einschätzung des Wertes der betreffenden Objekte und der Höhe des im Falle einer Kenntnisnahme durch Unbefugte eventuell entstehenden Schadens; Beschaffenheit und Lage des Gebäudes, in dem das System untergebracht ist; Ort, an dem sich das System innerhalb des Gebäudes befindet.

Notfallpläne

19. Es sind detaillierte Pläne auszuarbeiten, um im Falle eines örtlichen oder nationalen Notstands auf den Schutz von Verschlusssachen vorbereitet zu sein.

INFORMATIONSSICHERHEIT (INFOSEC)

20. INFOSEC betrifft die Festlegung und Anwendung von Sicherheitsmaßnahmen, mit denen in Kommunikations-, Informations- und sonstigen elektronischen Systemen bearbeitete, gespeicherte oder übermittelte Verschlusssachen davor geschützt werden sollen, versehentlich oder absichtlich in die Hände von Unbefugten zu gelangen bzw. ihre Integrität oder Verfügbarkeit zu verlieren. Es sind geeignete Gegenmaßnahmen zu ergreifen, um zu verhindern, dass unbefugte Nutzer Zugang zu EU-Informationen erhalten, befugten Nutzern der Zugang zu EU-Informationen verweigert wird oder es zu einer Verfälschung, unbefugten Änderung oder Löschung von EU-Informationen kommt.

MASSNAHMEN GEGEN SABOTAGE UND ANDERE FORMEN VORSÄTZLICHER BESCHÄDIGUNG

21. Vorsichtsmaßnahmen im Bereich des Objektschutzes zum Schutz wichtiger Einrichtungen, in denen Verschlusssachen untergebracht sind, sind die besten Sicherheitsgarantien gegen Sabotage und vorsätzliche Beschädigungen; eine Sicherheitsüberprüfung des Personals allein ist kein wirklicher Ersatz. Die zuständige einzelstaatliche Stelle hat die Aufgabe, Erkenntnisse über Spionage, Sabotage, Terrorismus und andere subversive Tätigkeiten zusammenzutragen.

WEITERGABE VON VERSCHLUSSSACHEN AN DRITTSTAATEN ODER INTERNATIONALE ORGANISATIONEN

22. Der Beschluss, vom Rat stammende EU-Verschlusssachen an einen Drittstaat oder eine internationale Organisation weiterzugeben, wird vom Rat gefasst. Stammen die Verschlusssachen, um deren Weitergabe ersucht wird, nicht vom Rat, so hat dieser zunächst die Zustimmung des Urhebers der Verschlusssachen einzuholen. Kann dieser Urheber nicht ermittelt werden, so trifft der Rat an seiner Stelle die Entscheidung.

23. Erhält der Rat Verschlusssachen von Drittstaaten, internationalen Organisationen oder sonstigen Dritten, so werden sie in einer ihrem Geheimhaltungsgrad angemessenen Weise nach Maßgabe der für EU-Verschlusssachen geltenden Standards dieser Vorschriften oder aber höherer Standards, falls diese von der die Verschlusssachen weitergebenden dritten Seite gefordert werden, geschützt. Gegenseitige Kontrollen können vereinbart werden.

24. Die vorstehend dargelegten Grundprinzipien werden gemäß den detaillierten Vorschriften des Teils II verwirklicht.

▼B

TEIL II

ABSCHNITT I

DIE ORGANISATION DER SICHERHEIT IM RAT DER EUROPÄISCHEN UNION

Der Generalsekretär/Hohe Vertreter

1. Der Generalsekretär/Hohe Vertreter

   a) führt das Sicherheitskonzept des Rates durch;

   b) befasst sich mit Sicherheitsproblemen, die der Rat oder seine zuständigen Gremien ihm vorlegen;

   c) prüft in enger Abstimmung mit den nationalen Sicherheitsbehörden (oder sonstigen geeigneten Behörden) der Mitgliedstaaten Fragen, die eine Änderung des Sicherheitskonzepts des Rates erforderlich machen. Anhang 1 enthält eine Liste der entsprechenden Behörden.

2. Der Generalsekretär/Hohe Vertreter ist insbesondere für Folgendes zuständig:

   a) er koordiniert alle die Tätigkeiten des Rates betreffenden Sicherheitsfragen;

   b) er ersucht die einzelnen Mitgliedstaaten bzw. verpflichtet gegebenenfalls die dezentralen EU-Einrichtungen, ein Zentralregister der als „TRÈS SECRET UE/EU TOP SECRET“ eingestuften Verschlusssachen anzulegen;

   c) er richtet an die hierfür benannten Behörden der Mitgliedstaaten Anträge auf Sicherheitsüberprüfung im Generalsekretariat des Rates beschäftigter Personen durch die jeweilige nationale Sicherheitsbehörde im Einklang mit Abschnitt VI;

   d) er ermittelt oder ordnet Ermittlungen an, wenn EU-Verschlusssachen Unbefugten zur Kenntnis gelangt sind und die Ursache hierfür dem ersten Anschein nach im Generalsekretariat des Rates oder in einer der dezentralen EU-Einrichtungen zu suchen ist;

   e) er ersucht die entsprechenden Sicherheitsbehörden um die Einleitung von Ermittlungen, wenn eine Kenntnisnahme von EU-Verschlusssachen durch Unbefugte außerhalb des Generalsekretariats des Rates oder der dezentralen EU-Einrichtungen erfolgt zu sein scheint, und koordiniert die Ermittlungen in den Fällen, in denen mehr als eine Sicherheitsbehörde beteiligt ist;

   f) er überprüft gemeinsam und im Einvernehmen mit den betreffenden nationalen Sicherheitsbehörden periodisch die Sicherheitsvorkehrungen zum Schutz von EU-Verschlusssachen in den Mitgliedstaaten;

   g) er unterhält enge Verbindungen zu allen betroffenen Sicherheitsbehörden, um für eine Gesamtkoordinierung der Sicherheitsmaßnahmen zu sorgen;

   h) er behält ständig das Sicherheitskonzept und die Sicherheitsverfahren des Rates im Auge und arbeitet gegebenenfalls entsprechende Empfehlungen aus. In diesem Zusammenhang legt er dem Rat den vom Sicherheitsbüro des Generalsekretariats des Rates erstellten jährlichen Inspektionsplan vor.

Der Sicherheitsausschuss des Rates

3. Es wird ein Sicherheitsausschuss eingesetzt. Er besteht aus Vertretern der nationalen Sicherheitsbehörden der einzelnen Mitgliedstaaten. Den Vorsitz im Ausschuss führt der Generalsekretär/Hohe Vertreter bzw. eine von ihm beauftragte Person. Vertreter dezentraler EU-Einrichtungen können eingeladen werden, wenn sie betreffende Fragen erörtert werden.

4. Der Sicherheitsausschuss tritt gemäß dem vom Rat erteilten Mandat auf Antrag des Generalsekretärs/Hohen Vertreters oder einer nationalen Sicherheitsbehörde zusammen. Er kann alle Sicherheitsfragen prüfen und bewerten, die mit der Arbeit des Rates zu tun haben, und dem Rat gegebenenfalls Empfehlungen vorlegen. Der Ausschuss kann dem Generalsekretär/Hohen Vertreter in Bezug auf die Tätigkeit des Generalsekretariats des Rates Empfehlungen zu Sicherheitsfragen vorlegen.

Das Sicherheitsbüro des Generalsekretariats des Rates

5. Dem Generalsekretär/Hohen Vertreter steht für die Wahrnehmung seiner unter den Nummern 1 und 2 genannten Aufgaben das Sicherheitsbüro des

▼B

Generalsekretariats des Rates für die Koordinierung, Überwachung und Durchführung von Sicherheitsmaßnahmen zur Verfügung.

6. Der Leiter des Sicherheitsbüros des Generalsekretariats des Rates ist der wichtigste Berater des Generalsekretärs/Hohen Vertreters in Sicherheitsfragen und zugleich Sekretär des Sicherheitsausschusses. In dieser Hinsicht leitet er die Aktualisierung der Sicherheitsvorschriften und koordiniert die Sicherheitsmaßnahmen zusammen mit den zuständigen Behörden der Mitgliedstaaten und gegebenenfalls mit internationalen Organisationen, die Sicherheitsabkommen mit dem Rat geschlossen haben. Er hat hierbei die Rolle eines Verbindungsbeamten.

7. Der Leiter des Sicherheitsbüros des Generalsekretariats des Rates ist für die Zulassung von IT-Systemen und -netzen im Generalsekretariat des Rates zuständig. Der Leiter des Sicherheitsbüros des Generalsekretariats des Rates und die zuständigen nationalen Sicherheitsbehörden entscheiden gegebenenfalls gemeinsam über die Zulassung von IT-Systemen und -netzen, die das Generalsekretariat des Rates, die Mitgliedstaaten, dezentrale EU-Einrichtungen und/oder Dritte (Staaten oder internationale Organisationen) umfassen.

Dezentrale EU-Einrichtungen

8. Jeder Leiter einer dezentralen EU-Einrichtung ist für die Anwendung der Sicherheitsvorschriften in seiner Einrichtung zuständig. Im Regelfall bestimmt er einen seiner Mitarbeiter als den ihm rechenschaftspflichtigen Verantwortlichen für diesen Bereich. Der betreffende Mitarbeiter wird zum Sicherheitsbeauftragten ernannt.

Mitgliedstaaten

9. Jeder Mitgliedstaat sollte eine für die Sicherheit von EU-Verschlusssachen zuständige nationale Sicherheitsbehörde benennen ([1]).

10. Innerhalb der Verwaltungsstruktur der einzelnen Mitgliedstaaten sollte die jeweilige nationale Sicherheitsbehörde für Folgendes zuständig sein:

   a) die Gewährleistung der Sicherheit von EU-Verschlusssachen, die von einer öffentlichen oder privaten Stelle oder Einrichtung ihres Landes im In- oder Ausland verwahrt werden;

   b) die Genehmigung der Anlegung von Registern für Verschlusssachen, die als „TRÈS SECRET UE/EU TOP SECRET“ eingestuft sind (diese Genehmigungsbefugnis kann auch auf den in einer Zentralregistratur tätigen Kontrollbeamten für als „TRÈS SECRET UE/EU TOP SECRET“ eingestufte Verschlusssachen übertragen werden);

   c) die periodische Überprüfung der Sicherheitsvorkehrungen für den Schutz von EU-Verschlusssachen;

   d) die Sorge dafür, dass alle in Stellen oder Einrichtungen ihres Landes beschäftigten In- und Ausländer, die Zugang zu als „TRÈS SECRET UE/EU TOP SECRET“, „SECRET UE“ oder „CONFIDENTIEL UE“ eingestuften EU-Verschlusssachen haben könnten, sicherheitsüberprüft werden;

   e) die Aufstellung der Sicherheitspläne, die für erforderlich gehalten werden, um zu verhindern, dass EU-Verschlusssachen in unbefugte Hände gelangen.

Gegenseitige Sicherheitsinspektionen

11. Das Sicherheitsbüro des Generalsekretariats des Rates und die jeweilige nationale Sicherheitsbehörde führen gemeinsam und im gegenseitigen Einvernehmen periodische Inspektionen der Sicherheitsvorkehrungen durch, die zum Schutz von EU-Verschlusssachen im Generalsekretariat des Rates und in den Ständigen Vertretungen der Mitgliedstaaten bei der Europäischen Union sowie in den Räumlichkeiten der Mitgliedstaaten in den Ratsgebäuden getroffen werden ([2]).

12. Das Sicherheitsbüro des Generalsekretariats des Rates oder auf Antrag des Generalsekretärs die nationale Sicherheitsbehörde des Gastlandes führt periodische Inspektionen der Sicherheitsvorkehrungen durch, die zum Schutz von EU-Verschlusssachen in den dezentralen EU-Einrichtungen getroffen werden.

([1]) Eine Liste der für die Sicherheit von EU-Verschlusssachen zuständigen nationalen Sicherheitsbehörden ist in Anhang 1 enthalten.

([2]) Unbeschadet des Wiener Übereinkommens von 1961 über diplomatische Beziehungen.

▼B

ABSCHNITT II

GEHEIMHALTUNGSGRADE UND KENNZEICHNUNGEN

GEHEIMHALTUNGSGRADE ([1])

Verschlusssachen werden wie folgt eingestuft:

1. „TRÈS SECRET UE/EU TOP SECRET“: Dieser Geheimhaltungsgrad findet nur auf Informationen und Material Anwendung, deren unbefugte Weitergabe den wesentlichen Interessen der Europäischen Union oder eines oder mehrerer ihrer Mitgliedstaaten einen äußerst schweren Schaden zufügen könnte.

2. „SECRET UE“: Dieser Geheimhaltungsgrad findet nur auf Informationen und Material Anwendung, deren unbefugte Weitergabe den wesentlichen Interessen der Europäischen Union oder eines oder mehrerer ihrer Mitgliedstaaten schweren Schaden zufügen könnte.

3. „CONFIDENTIEL UE“: Dieser Geheimhaltungsgrad findet auf Informationen und Material Anwendung, deren unbefugte Weitergabe den wesentlichen Interessen der Europäischen Union oder eines oder mehrerer ihrer Mitgliedstaaten schaden könnte.

4. „RESTREINT UE“: Dieser Geheimhaltungsgrad findet auf Informationen und Material Anwendung, deren unbefugte Weitergabe für die Interessen der Europäischen Union oder eines oder mehrerer ihrer Mitgliedstaaten nachteilig sein könnte.

KENNZEICHNUNGEN

5. Als Warnhinweis dienende Kennzeichnungen können benutzt werden, um den von einem Dokument abgedeckten Bereich oder eine besondere Verteilung gemäß dem Grundsatz „Kenntnis nur wenn nötig“ anzugeben.

6. Die Kennzeichnung „ESDP“/„PESD“ (= ESVP) ist auf Dokumenten und Kopien von Dokumenten anzubringen, die die Sicherheit und Verteidigung der Union oder eines oder mehrerer ihrer Mitgliedstaaten, oder die militärische oder nichtmilitärische Krisenbewältigung betreffen.

7. Bestimmte Dokumente, insbesondere Dokumente mit Bezug zu Informationstechnologie (IT)-Systemen, können mit einer zusätzlichen Kennzeichnung versehen werden, die in den entsprechenden Regelungen festgelegte weitere Sicherheitsmaßnahmen zur Folge hat.

ANBRINGUNG EINES HINWEISES AUF DEN GEHEIMHALTUNGSGRAD UND SONSTIGE KENNZEICHNUNGEN

8. Ein Hinweis auf den Geheimhaltungsgrad und sonstige Kennzeichnungen werden wie folgt angebracht:

   a) bei Dokumenten, die als „RESTREINT UE“ eingestuft werden, mit mechanischen oder elektronischen Mitteln;

   b) bei Dokumenten, die als „CONFIDENTIEL UE“ eingestuft werden, mit mechanischen Mitteln und von Hand oder durch Druck auf vorgestempeltem, registriertem Papier;

   c) auf Dokumenten, die als „SECRET UE“ oder „TRÈS SECRET UE/EU TOP SECRET“ eingestuft werden, mit mechanischen Mitteln und von Hand.

([1]) Anhang 2 enthält eine vergleichende Übersicht über die von der EU, der NATO, der WEU und den Mitgliedstaaten verwendeten Geheimhaltungsgrade.

▼B

ABSCHNITT III

REGELN FÜR DIE EINSTUFUNG ALS VERSCHLUSSSACHE

1. Informationen sind nur dann als Verschlusssachen einzustufen, wenn dies nötig ist. Der Geheimhaltungsgrad ist klar und korrekt anzugeben und nur so lange beizubehalten, wie die Informationen geschützt werden müssen.

2. Die Verantwortung für die Festlegung des Geheimhaltungsgrades einer Information und für jede anschließende Herabstufung oder Aufhebung des Geheimhaltungsgrades ([1]) liegt allein beim Urheber der Information.

   Einstufungen, Herabstufungen oder Aufhebungen des Geheimhaltungsgrades von Verschlusssachen werden von den Beamten und sonstigen Bediensteten des Generalsekretariats des Rates auf Anweisung ihres Generaldirektors oder mit dessen Zustimmung vorgenommen.

3. Die detaillierten Verfahren für die Behandlung von Verschlusssachen sind so ausgelegt, dass gewährleistet ist, dass die betreffenden Dokumente den ihrem Inhalt entsprechenden Schutz erhalten.

4. Die Zahl der Personen, die dazu ermächtigt sind, Dokumente des Geheimhaltungsgrades „TRÈS SECRET UE/EU TOP SECRET“ in Umlauf zu bringen, ist möglichst klein zu halten, und ihre Namen sind in einer Liste zu verzeichnen, die vom Generalsekretariat des Rates, von jedem Mitgliedstaat und erforderlichenfalls von jeder dezentralen EU-Einrichtung geführt wird.

ANWENDUNG DER GEHEIMHALTUNGSGRADE

5. Bei der Festlegung des Geheimhaltungsgrades eines Dokuments wird das Ausmaß der Schutzbedürftigkeit seines Inhalts entsprechend der Definition in Abschnitt II Nummern 1 bis 4 zugrunde gelegt. Es ist wichtig, dass die Einstufung korrekt vorgenommen wird und nur bei wirklichem Bedarf erfolgt. Dies gilt insbesondere für eine Einstufung als „TRÈS SECRET UE/EU TOP SECRET“.

6. Der Urheber eines Dokuments, das als Verschlusssache eingestuft werden soll, sollte sich der vorstehend genannten Regelungen bewusst sein und eine zu hohe oder zu niedrige Einstufung vermeiden.

   Eine hohe Einstufung scheint zwar auf den ersten Blick mehr Schutz für ein Dokument zu garantieren, doch kann die routinemäßige Vornahme einer zu hohen Einstufung dazu führen, dass das Vertrauen in die Gültigkeit des Einstufungssystems verloren geht.

   Andererseits sollten Dokumente nicht in der Absicht zu niedrig eingestuft werden, die mit ihrem Schutz verbundenen Zwänge zu vermeiden.

   Anhang 3 enthält einen praktischen Leitfaden für die Einstufung.

7. Einzelne Seiten, Abschnitte, Teile, Anhänge oder sonstige Anlagen eines Dokuments können eine unterschiedliche Einstufung erforderlich machen und sind entsprechend zu kennzeichnen. Als Geheimhaltungsgrad des Gesamtdokuments gilt der Geheimhaltungsgrad seines am höchsten eingestuften Teils.

8. Ein Begleitschreiben oder ein Übermittlungsvermerk ist so hoch einzustufen wie die am höchsten eingestufte Anlage. Der Urheber sollte klar angeben, welcher Geheimhaltungsgrad für das Begleitschreiben bzw. den Übermittlungsvermerk gilt, wenn ihm seine Anlagen nicht beigefügt sind.

HERABSTUFUNG UND AUFHEBUNG DES GEHEIMHALTUNSGRADES

9. EU-Verschlusssachen dürfen nur mit Genehmigung des Urhebers und erforderlichenfalls nach Erörterung mit den übrigen beteiligten Parteien herabgestuft werden; das Gleiche gilt für die Aufhebung des Geheimhaltungsgrades. Die Herabstufung oder die Aufhebung des Geheimhaltungsgrades ist schriftlich zu bestätigen. Dem Organ, dem Mitgliedstaat, dem Amt, der Nachfolgeorganisation oder der höheren Stelle, von dem bzw. der die Verschlusssache stammt, obliegt es, die Empfänger des Dokuments über die Änderung der Einstufung zu informieren, wobei letztere wiederum die weiteren Empfänger, denen sie das Original oder eine Kopie des Dokuments zugeleitet haben, davon zu unterrichten haben.

([1]) Unter Herabstufung ist die Einstufung in einen niedrigeren Geheimhaltungsgrad zu verstehen; Aufhebung des Geheimhaltungsgrades bedeutet Löschung jeder Geheimhaltungskennzeichnung.

▼B

10. Soweit möglich gibt die Stelle, von der das Dokument stammt, auf dem als Verschlusssache eingestuften Dokument den Zeitpunkt oder eine Frist an, ab dem/nach deren Ablauf die in dem Dokument enthaltenen Informationen herabgestuft werden können oder deren Geheimhaltungsgrad aufgehoben werden kann. Andernfalls überprüft sie die Dokumente spätestens alle fünf Jahre, um sicherzustellen, dass die ursprüngliche Einstufung nach wie vor erforderlich ist.

▼B

ABSCHNITT IV

MATERIELLER GEHEIMSCHUTZ

ALLGEMEINES

1. Hauptziel der Maßnahmen des materiellen Geheimschutzes ist es, zu verhindern, dass Unbefugte Zugang zu EU-Verschlusssachen erhalten.

SICHERHEITSANFORDERUNGEN

2. Alle Gebäude, Bereiche, Büros, Räume, Kommunikations- und Informationssysteme usw., in denen als EU-Verschlusssache eingestufte Informationen und/oder Material aufbewahrt werden und/oder in denen damit gearbeitet wird, sind durch geeignete Maßnahmen des materiellen Geheimschutzes zu sichern.

3. Bei der Festlegung des erforderlichen materiellen Geheimschutzniveaus ist allen relevanten Faktoren Rechnung zu tragen, wie beispielsweise

   a) der Einstufung der Informationen und/oder des Materials;

   b) der Menge und der Form (z. B. Papier, EDV-Datenträger) der verwahrten Informationen;

   c) der örtlichen Einschätzung der geheimdienstlichen Bedrohung, die gegen die EU, die Mitgliedstaaten und/oder andere Institutionen oder Dritte gerichtet ist, die EU-Verschlusssachen verwahren, sowie der Bedrohung insbesondere durch Sabotage, Terrorismus und andere subversive und/oder kriminelle Handlungen.

4. Die Maßnahmen des materiellen Geheimschutzes zielen darauf ab,

   a) das heimliche oder gewaltsame Eindringen unbefugter Personen von außen zu verhindern;

   b) von Tätigkeiten illoyaler Angehöriger des Personals (Spionage von innen) abzuschrecken beziehungsweise diese zu verhindern und aufzudecken;

   c) zu verhindern, dass Beamte und sonstige Bedienstete des Generalsekretariats des Rates, von Regierungsdienststellen der Mitgliedstaaten und/oder anderen Institutionen oder Dritte, die die betreffenden Kenntnisse nicht benötigen, Zugang zu EU-Verschlusssachen erhalten.

MASSNAHMEN DES MATERIELLEN GEHEIMSCHUTZES

Sicherheitsbereiche

5. Die Bereiche, in denen mit als „CONFIDENTIEL UE“ oder höher eingestuften Verschlusssachen gearbeitet wird oder in denen diese aufbewahrt werden, sind so zu gestalten und auszustatten, dass sie einer der nachstehenden Kategorien entsprechen:

   a) Sicherheitsbereich der Kategorie I: Bereich, in dem mit als „CONFIDENTIEL UE“ oder höher eingestuften Verschlusssachen gearbeitet wird oder in denen diese aufbewahrt werden, wobei das Betreten des Bereichs für alle praktischen Zwecke den Zugang zu den Verschlusssachen ermöglicht. Ein derartiger Bereich erfordert

      i) einen klar abgegrenzten und geschützten Raum mit vollständiger Ein- und Ausgangskontrolle;

      ii) ein Zutrittskontrollsystem, mit dem dafür gesorgt wird, dass nur die gehörig überprüften und eigens ermächtigten Personen den Bereich betreten können;

      iii) eine genaue Festlegung der Einstufung der Verschlusssachen, die in der Regel in dem Bereich verwahrt werden, d. h. der Informationen, die durch das Betreten des Bereichs zugänglich werden.

   b) Sicherheitsbereich der Kategorie II: Bereich, in dem mit als „CONFIDENTIEL UE“ oder höher eingestuften Verschlusssachen gearbeitet wird oder in denen diese aufbewahrt werden, wobei durch interne Kontrollen ein Schutz vor dem Zugang Unbefugter ermöglicht wird, beispielsweise Gebäude mit Büros, in denen regelmäßig mit als „CONFIDENTIEL UE“ eingestuften Verschlusssachen gearbeitet wird und in denen diese aufbewahrt werden. Ein derartiger Bereich erfordert

      i) einen klar abgegrenzten und geschützten Raum mit vollständiger Ein- und Ausgangskontrolle;

      ii) ein Zutrittskontrollsystem, mit dem dafür gesorgt wird, dass nur die gehörig überprüften und eigens ermächtigten Personen den Bereich unbegleitet betreten können. Bei allen anderen Personen ist eine Begleitung oder eine gleichwertige Kontrolle sicherzustellen, damit der Zugang Unbefugter zu EU-Verschlusssachen sowie ein unkon-

▼B

trolliertes Betreten von Bereichen, die technischen Sicherheitskontrollen unterliegen, verhindert werden.

Die Bereiche, die nicht rund um die Uhr von Dienst tuendem Personal besetzt sind, sind unmittelbar nach den üblichen Arbeitszeiten zu inspizieren, um sicherzustellen, dass die EU-Verschlusssachen ordnungsgemäß gesichert sind.

Verwaltungsbereich

6. Um die Sicherheitsbereiche der Kategorien I und II herum oder im Zugangsbereich zu ihnen kann ein Verwaltungsbereich mit geringerem Sicherheitsgrad vorgesehen werden. Ein derartiger Bereich erfordert einen deutlich abgegrenzten Raum, der die Kontrolle des Personals und der Fahrzeuge ermöglicht. In den Verwaltungsbereichen darf nur mit als „RESTREINT UE“ eingestuften Verschlusssachen gearbeitet werden und es dürfen auch nur diese Verschlusssachen dort aufbewahrt werden.

Eingangs- und Ausgangskontrollen

7. Das Betreten der Sicherheitsbereiche der Kategorien I und II wird mittels eines Berechtigungsausweises oder eines Systems zur persönlichen Identifizierung des ständigen Personals kontrolliert. Ferner wird ein Kontrollsystem für Besucher eingerichtet, damit der Zugang Unbefugter zu EU-Verschlusssachen verhindert werden kann. Eine Regelung mit Berechtigungsausweisen kann durch eine automatisierte Erkennung unterstützt werden, die als Ergänzung zum Einsatz des Personals des Sicherheitsdienstes zu verstehen ist, diesen aber nicht vollständig ersetzen kann. Eine Änderung in der Einschätzung der Bedrohungslage kann eine Verschärfung der Ein- und Ausgangskontrollmaßnahmen zur Folge haben, beispielsweise anlässlich des Besuchs hochrangiger Persönlichkeiten.

Kontrollgänge

8. In Sicherheitsbereichen der Kategorien I und II sind außerhalb der normalen Arbeitszeiten Kontrollgänge durchzuführen, um das Eigentum der EU vor Kenntnisnahme durch Unbefugte, Beschädigung oder Verluste zu schützen. Die Häufigkeit der Kontrollgänge richtet sich nach den örtlichen Gegebenheiten, sie sollten aber in der Regel alle zwei Stunden stattfinden.

Sicherheitsbehältnisse und Tresorräume

9. Zur Aufbewahrung von EU-Verschlusssachen werden drei Arten von Behältnissen verwendet:

   — Typ A: Behältnisse, die zur Aufbewahrung von als „TRÈS SECRET UE/EU TOP SECRET“ eingestuften Verschlusssachen in Sicherheitsbereichen der Kategorie I oder II auf nationaler Ebene zugelassen sind;

   — Typ B: Behältnisse, die zur Aufbewahrung von als „SECRET UE“ und „CONFIDENTIEL UE“ eingestuften Verschlusssachen in Sicherheitsbereichen der Kategorie I oder II auf nationaler Ebene zugelassen sind;

   — Typ C: Büromöbel, die ausschließlich für die Aufbewahrung von als „RESTREINT UE“ eingestuften Verschlusssachen geeignet sind.

10. In den in einem Sicherheitsbereich der Kategorie I oder II eingebauten Tresorräumen und in allen Sicherheitsbereichen der Kategorie I, wo als „CONFIDENTIEL UE“ und höher eingestufte Verschlusssachen in offenen Regalen aufbewahrt werden oder auf Karten, Plänen usw. sichtbar sind, werden Wände, Böden und Decken, Türen einschließlich der Schlösser von einer nationalen Sicherheitsbehörde geprüft, um festzustellen, dass sie einen Schutz bieten, der dem Typ des Sicherheitsbehältnisses entspricht, der für die Aufbewahrung von Verschlusssachen desselben Geheimhaltungsgrades zugelassen ist.

Schlösser

11. Die Schlösser der Sicherheitsbehältnisse und Tresorräume, in denen EU-Verschlusssachen aufbewahrt werden, müssen folgende Anforderungen erfüllen:

   — Gruppe A: sie müssen auf nationaler Ebene für Behältnisse vom Typ A zugelassen sein;

   — Gruppe B: sie müssen auf nationaler Ebene für Behältnisse vom Typ B zugelassen sein;

   — Gruppe C: sie müssen ausschließlich für Büromöbel vom Typ C geeignet sein.

▼B

Kontrolle der Schlüssel und Kombinationen

12. Die Schlüssel von Sicherheitsbehältnissen dürfen nicht aus dem Bürogebäude entfernt werden. Die Kombinationen für Sicherheitsbehältnisse sind von den Personen, die sie kennen müssen, auswendig zu lernen. Damit sie im Notfall benutzt werden können, ist der Geheimschutzbeauftragte der betreffenden Stelle für die Aufbewahrung der Ersatzschlüssel und die schriftliche Registrierung aller Kombinationen verantwortlich; letztere sind einzeln in versiegelten, undurchsichtigen Umschlägen aufzubewahren. Die Arbeitsschlüssel, die Ersatzschlüssel und die Kombinationen sind in gesonderten Sicherheitsbehältnissen aufzubewahren. Für diese Schlüssel und Kombinationen ist kein geringerer Sicherheitsschutz vorzusehen als für das Material, zu dem sie den Zugang ermöglichen.

13. Der Kreis der Personen, die die Kombinationen der Sicherheitsbehältnisse kennen, ist so weit wie möglich zu begrenzen. Die Kombinationen sind zu ändern

    a) bei Entgegennahme eines neuen Behälters;

    b) bei jedem Benutzerwechsel;

    c) bei tatsächlicher oder vermuteter Kenntnisnahme durch Unbefugte;

    d) vorzugsweise alle sechs Monate und mindestens alle zwölf Monate.

Intrusionsmeldeanlagen

14. Kommen zum Schutz von EU-Verschlusssachen Alarmanlagen, hauseigene Fernsehsysteme und andere elektrische Vorrichtungen zum Einsatz, so ist eine Notstromversorgung vorzusehen, um bei Ausfall der Hauptstromversorgung den ununterbrochenen Betrieb der Anlagen sicherzustellen. Ein weiteres grundlegendes Erfordernis ist das Auslösen eines für das Überwachungspersonal bestimmten Alarmsignals oder anderen verlässlichen Signals bei Funktionsstörungen dieser Anlagen oder Manipulationen an ihnen.

Zugelassene Ausrüstung

15. Die nationalen Sicherheitsbehörden unterhalten aktualisierte, nach Typ und Modell gegliederte Verzeichnisse der aus eigenen oder aus bilateralen Quellen stammenden Sicherheitsausrüstung, die sie für den unmittelbaren oder mittelbaren Schutz von Verschlusssachen unter verschiedenen genau bezeichneten Voraussetzungen und Bedingungen zugelassen haben. Das Sicherheitsbüro des Generalsekretariats des Rates unterhält ein entsprechendes Verzeichnis, das unter anderem auf den von den nationalen Sicherheitsbehörden mitgeteilten Informationen beruht. Die dezentralen EU-Einrichtungen konsultieren das Sicherheitsbüro des Generalsekretariats des Rates und gegebenenfalls die nationale Sicherheitsbehörde ihres Sitzmitgliedstaats, bevor sie derartige Ausrüstungen erwerben.

Materieller Geheimschutz für Kopier- und Faxgeräte

16. Für Kopier- und Faxgeräte ist im erforderlichen Maß durch Maßnahmen des materiellen Geheimschutzes dafür zu sorgen, dass sie lediglich von befugten Personen verwendet werden können und dass alle Verschlusssachen einer ordnungsgemäßen Überwachung unterliegen.

SICHT- UND ABHÖRSCHUTZ

Sichtschutz

17. Es sind alle geeigneten Maßnahmen zu treffen, damit bei Tag und bei Nacht gewährleistet ist, dass EU-Verschlusssachen nicht — auch nicht versehentlich — von Unbefugten eingesehen werden können.

Abhörschutz

18. Die Büroräume oder Bereiche, in denen regelmäßig über als „SECRET UE“ und höher eingestufte Verschlusssachen gesprochen wird, sind bei entsprechendem Risiko gegen Ab- und Mithören zu schützen. Für die Einschätzung des Risikos ist die jeweilige Sicherheitsbehörde zuständig, die erforderlichenfalls zuvor die betreffenden nationalen Sicherheitsbehörden zurate zieht.

19. Zur Festlegung der Schutzmaßnahmen für mithörgefährdete Bereiche (beispielsweise Schalldämpfung von Wänden, Türen, Böden und Decken, Lautstärkemessung) in Bezug auf Mit- bzw. Abhörgefahr bzw. abhörgefährdete Bereiche (beispielsweise Suche nach Mikrofonen), kann das Sicherheitsbüro des Generalsekretariats des Rates die nationalen Sicherheitsbehörden um Unterstützung durch Sachverständige ersuchen. Die Sicherheitsbeauftragten der dezentralen EU-Stellen können darum ersuchen, dass das Sicherheitsbüro des Generalsekretariats des Rates technische Kontrollen durchführt und/oder die nationalen Sicherheitsbehörden sie mit Sachverständigen unterstützen.

▼B

20. Ebenso können die für die technische Sicherheit zuständigen Sachverständigen der nationalen Sicherheitsbehörden erforderlichenfalls die Telekommunikationseinrichtungen und die elektrischen oder elektronischen Büromaschinen aller Art, die in den Sitzungen des Geheimhaltungsgrades „SECRET UE“ und höher verwendet werden, auf Ersuchen des zuständigen Sicherheitsbeauftragten überprüfen.

HOCHSICHERHEITSZONEN

21. Bestimmte Bereiche können als Hochsicherheitszonen ausgewiesen werden. Hier findet eine besondere Zutrittskontrolle statt. Diese Zonen bleiben nach einem zugelassenen Verfahren verschlossen, wenn sie nicht besetzt sind, und alle Schlüssel sind als Sicherheitsschlüssel zu behandeln. Diese Zonen unterliegen regelmäßigen Objektschutzkontrollen, die auch durchgeführt werden, wenn festgestellt oder vermutet wird, dass die Zonen ohne Genehmigung betreten wurden.

22. Es wird eine detaillierte Bestandsaufnahme der Geräte und Möbel vorgenommen, um deren Platzveränderungen zu überwachen. Kein Möbelstück oder Gerät wird in eine dieser Zonen verbracht, bevor es nicht durch Sicherheitspersonal, das für das Aufspüren von Abhörvorrichtungen besonders geschult ist, sorgfältig kontrolliert worden ist. In der Regel sollten in Hochsicherheitszonen möglichst keine Telekommunikationsverbindungen installiert werden.

▼B

ABSCHNITT V

ALLGEMEINE BESTIMMUNGEN ZU DEM GRUNDSATZ „KENNTNIS NUR WENN NÖTIG“ UND DER SICHERHEITSÜBERPRÜFUNG

1. Der Zugang zu EU-Verschlusssachen wird nur Personen gestattet, die Kenntnis von ihnen haben müssen, um die ihnen übertragenen Aufgaben oder Aufträge erfüllen zu können. Der Zugang zu als „TRÈS SECRET UE/EU TOP SECRET“, „SECRET UE“ und „CONFIDENTIEL UE“ eingestuften Verschlusssachen wird nur Personen gestattet, die der entsprechenden Sicherheitsüberprüfung unterzogen worden sind.

2. Für die Entscheidung darüber, wer Kenntnis haben muss, sind das Generalsekretariat des Rates, die dezentralen EU-Einrichtungen sowie die Dienststelle oder Behörde des Mitgliedstaats, in der die betreffende Person beschäftigt werden soll, entsprechend den Anforderungen der jeweiligen Aufgabe verantwortlich.

3. Für die Überprüfung von Personen ist der Arbeitgeber des Beamten nach Maßgabe der einschlägigen geltenden Verfahren verantwortlich. Für die Beamten und sonstigen Bediensteten des Generalsekretariats des Rates ist das Überprüfungsverfahren in Abschnitt VI geregelt.

   Am Ende des Verfahrens wird eine „Sicherheitsunbedenklichkeitsbescheinigung“ ausgestellt, in dem der Geheimhaltungsgrad der Verschlusssachen, zu denen die überprüfte Person Zugang erhalten kann, und das Ende der Gültigkeitsdauer der Bescheinigung angegeben werden.

   Eine Sicherheitsunbedenklichkeitsbescheinigung für einen bestimmten Geheimhaltungsgrad kann den Inhaber zum Zugang zu Informationen eines niedrigeren Geheimhaltungsgrades berechtigen.

4. Personen, bei denen es sich nicht um Beamte oder sonstige Bedienstete des Generalsekretariats des Rates oder der Mitgliedstaaten handelt, z. B. Mitglieder, Beamte oder Bedienstete von EU-Institutionen, mit denen möglicherweise EU-Verschlusssachen erörtert werden müssen oder die möglicherweise Einblick in diese erhalten müssen, müssen einer Sicherheitsüberprüfung in Bezug auf EU-Verschlusssachen unterzogen und über ihre Verantwortung für die Sicherheit belehrt worden sein. Die gleiche Regel gilt unter vergleichbaren Umständen für externe Auftragnehmer, Sachverständige oder Berater.

BESONDERE VORSCHRIFTEN FÜR DEN ZUGANG ZU ALS „TRÈS SECRET UE/EU TOP SECRET“ EINGESTUFTEN VERSCHLUSSSACHEN

5. Alle Personen, die Zugang zu als „TRÈS SECRET UE/EU TOP SECRET“ eingestuften Verschlusssachen benötigen, müssen zunächst einer Sicherheitsüberprüfung in Bezug auf den Zugang zu den betreffenden Verschlusssachen unterzogen werden.

6. Alle Personen, die Zugang zu als „TRÈS SECRET UE/EU TOP SECRET“ eingestuften Verschlusssachen benötigen, sind von ihren Abteilungsleitern zu benennen und ihre Namen sind in das einschlägige „TRÈS SECRET UE/EU TOP SECRET“-Register einzutragen.

7. Bevor diesen Personen der Zugang zu als „TRÈS SECRET UE/EU TOP SECRET“ eingestuften Verschlusssachen gewährt wird, müssen sie eine Urkunde des Inhalts unterzeichnen, dass sie über die Sicherheitsverfahren des Rates belehrt worden sind, sich ihrer besonderen Verantwortung für den Schutz von als „TRÈS SECRET UE/EU TOP SECRET“ eingestuften Verschlusssachen und der Folgen vollständig bewusst sind, die in den EU-Vorschriften und den einzelstaatlichen Rechts- und Verwaltungsvorschriften für den Fall vorgesehen sind, dass Verschlusssachen durch Vorsatz oder durch Fahrlässigkeit in die Hände Unbefugter gelangen.

8. Wenn Personen in Sitzungen Zugang zu als „TRÈS SECRET UE/EU TOP SECRET“ eingestuften Verschlusssachen erhalten, so teilt der Kontrollbeamte der Dienststelle oder des Gremiums, bei der bzw. dem die Betreffenden beschäftigt sind, der die Sitzung veranstaltenden Stelle mit, dass die betreffenden Personen die entsprechende Ermächtigung besitzen.

9. Die Namen aller Personen, die nicht mehr für Aufgaben eingesetzt werden, bei denen sie über den Zugang zu als „TRÈS SECRET UE/EU TOP SECRET“ eingestuften Verschlusssachen verfügen müssen, werden aus dem „TRÈS SECRET UE/EU TOP SECRET“-Verzeichnis gestrichen. Ferner werden alle betreffenden Personen erneut auf ihre besondere Verantwortung für den Schutz von als „TRÈS SECRET UE/EU TOP SECRET“ eingestuften Verschlusssachen belehrt. Sie haben ferner eine Erklärung zu unterzeichnen, wonach sie ihre Kenntnisse über als „TRÈS SECRET UE/

▼B

EU TOP SECRET“ eingestufte Verschlusssachen weder verwenden noch weitergeben werden.

BESONDERE VORSCHRIFTEN FÜR DEN ZUGANG ZU ALS „SECRET UE“ UND „CONFIDENTIEL UE“ EINGESTUFTEN VERSCHLUSSSACHEN

10. Alle Personen, die Zugang zu als „SECRET UE“ oder „CONFIDENTIEL UE“ eingestuften Verschlusssachen benötigen, müssen zunächst einer Sicherheitsüberprüfung in Bezug auf den Zugang zu den betreffenden Verschlusssachen unterzogen werden.

11. Alle Personen, die Zugang zu als „SECRET UE“ oder „CONFIDENTIEL UE“ eingestuften Verschlusssachen benötigen, müssen über die entsprechenden Sicherheitsregelungen unterrichtet werden und sich der Folgen fahrlässigen Handelns bewusst sein.

12. Wenn Personen in Sitzungen Zugang zu als „SECRET UE“ oder „CONFIDENTIEL UE“ eingestuften Verschlusssachen erhalten, so teilt der Kontrollbeamte der Dienststelle oder des Gremiums, bei der bzw. dem die Betreffenden beschäftigt sind, der die Sitzung veranstaltenden Stelle mit, dass die betreffenden Personen die entsprechende Ermächtigung besitzen.

BESONDERE VORSCHRIFTEN FÜR DEN ZUGANG ZU ALS „RESTREINT UE“ EINGESTUFTEN VERSCHLUSSSACHEN

13. Alle Personen, die Zugang zu als „RESTREINT UE“ eingestuften Verschlusssachen haben, werden auf diese Sicherheitsvorschriften und die Folgen fahrlässigen Handelns aufmerksam gemacht.

WEITERGABE

14. Wird ein Angehöriger des Personals von einem Dienstposten, der mit der Arbeit mit EU-Verschlusssachen verbunden ist, wegversetzt, so achtet die Registratur darauf, dass die betreffenden Verschlusssachen ordnungsgemäß von dem ausscheidenden an den eintretenden Beamten weitergegeben werden.

BESONDERE ANWEISUNGEN

15. Personen, die mit EU-Verschlusssachen arbeiten müssen, sollten bei Aufnahme ihrer Tätigkeit und danach in regelmäßigen Abständen auf Folgendes hingewiesen werden:

    a) die mögliche Gefährdung der Sicherheit durch indiskrete Gespräche;

    b) die in den Beziehungen zur Presse zu treffenden Vorsichtsmaßnahmen;

    c) die Bedrohung für EU-Verschlusssachen und -tätigkeiten durch die gegen die EU und ihre Mitgliedstaaten gerichteten nachrichtendienstlichen Tätigkeiten;

    d) die Verpflichtung, die zuständigen Sicherheitsbehörden unverzüglich über jeden Annäherungsversuch oder jede Handlungsweise, bei denen ein Verdacht auf Spionage entsteht, sowie über alle ungewöhnlichen Umstände in Bezug auf die Sicherheit zu unterrichten.

16. Alle Personen, die gewöhnlich häufige Kontakte mit Vertretern von Ländern haben, deren Nachrichtendienste in Bezug auf EU-Verschlusssachen und Tätigkeiten gegen die EU und ihre Mitgliedstaaten arbeiten, sind über die Techniken zu belehren, von denen bekannt ist, dass sich die einzelnen Nachrichtendienste ihrer bedienen.

17. Es bestehen keine Sicherheitsregelungen des Rates für private Reisen der zum Zugang zu EU-Verschlusssachen ermächtigten Personen nach irgendeinem Zielland. Die zuständigen Sicherheitsbehörden werden jedoch die Beamten und sonstigen Bediensteten, für die sie zuständig sind, über Reiseregelungen unterrichten, denen sie möglicherweise unterliegen. Die Geheimschutzbeauftragten sind dafür verantwortlich, für das betroffene Personal Sitzungen zur Auffrischung der Kenntnisse über die betreffenden besonderen Anweisungen zu veranstalten.

▼B

ABSCHNITT VI

VERFAHREN FÜR DIE SICHERHEITSÜBERPRÜFUNG VON BEAMTEN UND SONSTIGEN BEDIENSTETEN DES GENERALSEKRETARIATS DES RATES

1. Nur Beamte und sonstige Bedienstete des Generalsekretariats des Rates oder andere beim Generalsekretariat des Rates tätige Personen, die aufgrund ihrer Aufgabenbereiche und dienstlicher Erfordernisse von den vom Rat verwahrten Verschlusssachen Kenntnis nehmen müssen, oder sie zu bearbeiten haben, erhalten Zugang zu diesen Verschlusssachen.

2. Um Zugang zu den als „TRÈS SECRET UE/EU TOP SECRET“, „SECRET UE“ und „CONFIDENTIEL UE“ eingestuften Verschlusssachen zu erhalten, müssen die in Nummer 1 genannten Personen hierzu nach dem Verfahren der Nummern 4 und 5 ermächtigt worden sein.

3. Die Ermächtigung wird nur den Personen erteilt, die durch die zuständigen nationalen Behörden der Mitgliedstaaten (nationale Sicherheitsbehörden) einer Sicherheitsüberprüfung nach dem in den Nummern 6 bis 10 beschriebenen Verfahren unterzogen worden sind.

4. Die Erteilung der Ermächtigungen gemäß den Nummern 1, 2 und 3 obliegt der Anstellungsbehörde im Sinne von Artikel 2 Absatz 1 des Personalstatuts.

   Die Anstellungsbehörde erteilt die Ermächtigung nach Einholung der Stellungnahme der zuständigen nationalen Sicherheitsbehörden der Mitgliedstaaten auf der Grundlage der gemäß den Nummern 6 bis 12 durchgeführten Sicherheitsüberprüfung.

5. Die Ermächtigung, die eine Geltungsdauer von fünf Jahren hat, erlischt, wenn die betreffende Person die Aufgaben, die die Erteilung der Ermächtigung gerechtfertigt haben, nicht mehr wahrnimmt. Sie kann von der Anstellungsbehörde nach dem Verfahren der Nummer 4 erneuert werden.

   Die Ermächtigung wird dem Betreffenden von der Anstellungsbehörde entzogen, wenn ihrer Ansicht nach hierzu Grund besteht. Die Entzugsverfügung wird der betreffenden Person, die beantragen kann, von der Anstellungsbehörde gehört zu werden, sowie der zuständigen nationalen Behörde mitgeteilt.

6. Durch die Sicherheitsüberprüfung soll gewährleistet werden, dass es keine Einwände dagegen gibt, dass die betreffende Person Zugang zu den vom Rat verwahrten Verschlusssachen erhalten kann.

7. Die Sicherheitsüberprüfung wird unter Mitwirkung der betreffenden Person auf Ersuchen der Anstellungsbehörde von den zuständigen nationalen Behörden desjenigen Mitgliedstaats vorgenommen, dessen Staatsangehörigkeit die zu ermächtigende Person besitzt. Hat die betreffende Person ihren Wohnsitz in einem anderen Mitgliedstaat, so können die betreffenden nationalen Behörden sich die Mitwirkung der Behörden des Wohnsitzstaats sichern.

8. Die betreffende Person hat im Hinblick auf die Sicherheitsüberprüfung eine Sicherheitserklärung auszufüllen.

9. Die Anstellungsbehörde benennt in ihrem Ersuchen die Art und den Geheimhaltungsgrad der Informationen, zu denen die betreffende Person Zugang erhalten soll, damit die zuständigen nationalen Behörden das Sicherheitsüberprüfungsverfahren durchführen und zu der der betreffenden Person zu erteilenden Ermächtigungsstufe Stellung nehmen können.

10. Für den gesamten Ablauf und die Ergebnisse des Sicherheitsüberprüfungsverfahrens gelten die einschlägigen Vorschriften und Regelungen des betreffenden Mitgliedstaats, einschließlich der Vorschriften und Regelungen für etwaige Rechtsbehelfe.

11. Bei befürwortender Stellungnahme der zuständigen nationalen Behörden der Mitgliedstaaten kann die Anstellungsbehörde der betreffenden Person die Ermächtigung erteilen.

12. Bei ablehnender Stellungnahme der zuständigen nationalen Behörden wird diese Ablehnung der betreffenden Person mitgeteilt, die beantragen kann, von der Anstellungsbehörde gehört zu werden. Die Anstellungsbehörde kann, wenn sie dies für erforderlich hält, bei den zuständigen nationalen Behörden um weitere Auskünfte, die diese zu geben vermögen, nachsuchen. Bei Bestätigung der ablehnenden Stellungnahme kann die Ermächtigung nicht erteilt werden.

▼B

13. Jede ermächtigte Person im Sinne der Nummern 4 und 5 erhält zum Zeitpunkt der Ermächtigung und danach in regelmäßigen Abständen die gebotenen Anweisungen zum Schutz der Verschlusssachen und zu den Verfahren zur Sicherstellung dieses Schutzes. Sie unterzeichnet eine Erklärung, mit der sie den Erhalt dieser Anweisungen bestätigt und sich zu ihrer Einhaltung verpflichtet.

14. Die Anstellungsbehörde ergreift alle erforderlichen Maßnahmen für die Durchführung dieses Abschnitts, insbesondere hinsichtlich der Regelung für den Zugang zum Verzeichnis der ermächtigten Personen.

15. Ausnahmsweise kann die Anstellungsbehörde aufgrund dienstlicher Erfordernisse, nachdem sie die zuständigen nationalen Behörden hiervon im Voraus unterrichtet hat und diese binnen einem Monat nicht dazu Stellung genommen haben, auch eine einstweilige Ermächtigung für höchstens sechs Monate erteilen, bis ihr die Ergebnisse der Sicherheitsüberprüfung nach Nummer 7 vorliegen.

16. Die so erteilten vorläufigen und befristeten Ermächtigungen berechtigen nicht zum Zugang zu als „TRÈS SECRET UE/EU TOP SECRET“ eingestuften Verschlusssachen; der Zugang wird auf die Beamten beschränkt, bei denen tatsächlich eine Sicherheitsüberprüfung gemäß Nummer 7 mit befürwortender Stellungnahme abgeschlossen worden ist. Bis die Ergebnisse der Sicherheitsüberprüfung vorliegen, können die Beamten, die die Ermächtigungsstufe „TRÈS SECRET UE/EU TOP SECRET“ erhalten sollen, vorläufig und befristet zum Zugang zu als „SECRET UE“ oder niedriger eingestuften Verschlusssachen ermächtigt werden.

▼B

ABSCHNITT VII

HERSTELLUNG, VERTEILUNG, ÜBERMITTLUNG, AUFBEWAHRUNG UND VERNICHTUNG VON EU-VERSCHLUSSSACHEN

Inhalt

▼B

Allgemeine Bestimmungen

Dieser Abschnitt enthält die Maßnahmen, die bei der Herstellung, Verteilung, Übermittlung, Aufbewahrung und Vernichtung von als EU-Verschlusssachen eingestuften Dokumenten im Sinne von Nummer 3 Buchstabe a) der in Teil I dieser Sicherheitsvorschriften enthaltenen Grundprinzipien und Mindeststandards für die Sicherheit zu treffen sind. Er ist als Grundlage heranzuziehen, wenn diese Maßnahmen für sonstiges als EU-Verschlusssache eingestuftes Material unter Berücksichtigung der Art des jeweils betroffenen Materials in jedem Einzelfall angepasst werden.

Kapitel I

Herstellung und Verteilung von EU-Verschlusssachen

HERSTELLUNG

1. Die EU-Geheimhaltungsgrade und sonstigen Kennzeichnungen sind in der in Abschnitt II angegebenen Weise oben und unten in der Mitte auf jeder Seite anzubringen, wobei jede Seite zu nummerieren ist. Auf jeder EU-Verschlusssache sind ein Aktenzeichen und ein Datum anzugeben. Im Falle von Dokumenten der Geheimhaltungsgrade „TRÈS SECRET UE/EU TOP SECRET“ und „SECRET UE“ muss das Aktenzeichen auf jeder Seite erscheinen. Werden sie in mehreren Ausfertigungen verteilt, so erhält jede Ausfertigung eine eigene Nummer, die auf der ersten Seite zusammen mit der Gesamtzahl der Seiten anzugeben ist. Alle Anhänge und Anlagen sind auf der ersten Seite von Dokumenten aufzulisten, die als „CONFIDENTIEL UE“ oder höher eingestuft werden.

2. Dokumente, die als „CONFIDENTIEL UE “ oder höher eingestuft werden, dürfen — außer in dem in Nummer 27 beschriebenen Sonderfall — nur von Personen maschinegeschrieben, übersetzt, archiviert, fotokopiert und auf Magnetband oder Mikrofiche gespeichert werden, die eine zumindest dem Geheimhaltungsgrad des betreffenden Dokuments entsprechende Zugangsermächtigung zu EU-Verschlusssachen haben.

   Abschnitt XI enthält die Vorschriften für die Erstellung von Verschlusssachen mit Hilfe eines Computers.

VERTEILUNG

3. EU-Verschlusssachen dürfen nur an Personen verteilt werden, für die deren Kenntnis nötig ist und die in entsprechender Weise sicherheitsüberprüft worden sind. Der Urheber bestimmt die Empfänger der erstmaligen Verteilung.

4. Dokumente des Geheimhaltungsgrades „TRÈS SECRET UE/EU TOP SECRET“ werden über „TRÈS SECRET UE/EU TOP SECRET“-Registraturen verteilt (siehe Abschnitt VIII). Im Falle als „TRÈS SECRET UE/EU TOP SECRET“ eingestufter Mitteilungen kann die zuständige Registratur dem Leiter des Kommunikationszentrums gestatten, die in der Liste der Empfänger angegebene Anzahl von Ausfertigungen zu erstellen.

5. Als „SECRET UE“ oder niedriger eingestufte Dokumente können vom Erstempfänger an weitere Empfänger, für die deren Kenntnis nötig ist, weiter gegeben werden. Die Stellen, von denen die Verschlusssachen stammen, können allerdings von ihnen gewünschte Einschränkungen bei der Verteilung mitteilen. In diesem Fall dürfen die Empfänger die Dokumente nur mit der Genehmigung der Stellen, von denen sie stammen, weiter geben.

6. Ein- und Ausgang jedes als „CONFIDENTIEL UE“ oder höher eingestuften Dokuments sind von der Registratur jeder Einrichtung, die dieses Dokument empfängt, zu verzeichnen. Die Angaben, die hierbei zu erfassen sind (Aktenzeichen, Datum und gegebenenfalls Nummer der Ausfertigung) müssen eine Identifizierung des Dokuments ermöglichen und sind in einem Dienstbuch oder in einem besonders geschützten Computermedium festzuhalten.

Kapitel II

Übermittlung von EU-Verschlusssachen

VERSAND

7. Als „CONFIDENTIEL UE“ oder höher eingestufte Dokumente sind in einem doppelten, widerstandsfähigen und undurchsichtigen Umschlag zu übermitteln. Auf dem inneren Umschlag sind der entsprechende EU-Geheimhaltungsgrad sowie möglichst die vollständige Amtsbezeichnung und Anschrift des Empfängers anzugeben.

▼B

8. Nur der Registraturkontrollbeamte oder sein Stellvertreter darf den inneren Umschlag öffnen und den Empfang der übermittelten Verschlusssachen bestätigen, es sei denn, der Umschlag ist ausdrücklich an einen bestimmten Empfänger gerichtet. In diesem Fall vermerkt die zuständige Registratur den Eingang des Umschlags und nur der genannte Empfänger darf den inneren Umschlag öffnen und den Empfang der darin enthaltenen Verschlusssachen bestätigen.

9. In dem inneren Umschlag ist eine Empfangsbestätigung beizulegen. In dieser Bestätigung, die nicht als Verschlusssache eingestuft wird, sind Aktenzeichen, Datum und die Nummer der Ausfertigung der Verschlusssache, niemals jedoch deren Betreff, anzugeben.

10. Der innere Umschlag wird in einen Außenumschlag gelegt, der für Empfangszwecke eine Versandnummer erhält. Der Geheimhaltungsgrad darf unter keinen Umständen auf dem Außenumschlag erscheinen.

11. Bei als „CONFIDENTIEL UE“ oder höher eingestuften Dokumenten ist Kurieren und Boten eine Empfangsbestätigung auszustellen, auf der die Versandnummern der übermittelten Versandstücke angegeben sind.

ÜBERMITTLUNG INNERHALB EINES GEBÄUDES ODER GEBÄUDEKOMPLEXES

12. Innerhalb eines bestimmten Gebäudes oder Gebäudekomplexes dürfen als Verschlusssachen eingestufte Dokumente in einem versiegelten Umschlag, der nur den Namen des Empfängers trägt, befördert werden, sofern die Beförderung durch eine für den betreffenden Geheimhaltungsgrad ermächtigte Person erfolgt.

ÜBERMITTLUNG VON EU-DOKUMENTEN INNERHALB EIN- UND DESSELBEN LANDES

13. Innerhalb ein- und desselben Landes sollten „TRÈS SECRET UE/EU TOP SECRET“-Dokumente nur unter Zuhilfenahme offizieller Kurierdienste oder durch Personen übermittelt werden, die eine Zugangsermächtigung zu als „TRÈS SECRET UE/EU TOP SECRET“ eingestuften Verschlusssachen haben.

14. Wird zur Übermittlung eines als „TRÈS SECRET UE/EU TOP SECRET“ eingestuften Dokuments an einen Empfänger außerhalb desselben Gebäudes oder Gebäudekomplexes ein Kurierdienst verwendet, so sind die Bestimmungen über den Versand und die Empfangsbestätigung in diesem Kapitel einzuhalten. Die Zustelldienste sind personell so auszustatten, dass gewährleistet ist, dass sich Versandstücke mit als „TRÈS SECRET UE/EU TOP SECRET“ eingestuften Dokumenten jederzeit unter der direkten Aufsicht eines verantwortlichen Beamten befinden.

15. In Ausnahmefällen können Beamte, die nicht Boten sind, als „TRÈS SECRET UE/EU TOP SECRET“ eingestufte Dokumente außerhalb des Gebäudes oder Gebäudekomplexes zur Benutzung vor Ort anlässlich von Sitzungen oder Erörterungen mitnehmen, vorausgesetzt, dass

    a) der betreffende Beamte zum Zugang zu diesen als „TRÈS SECRET UE/EU TOP SECRET“ eingestuften Dokumenten ermächtigt ist;

    b) die Form der Beförderung den einzelstaatlichen Vorschriften für die Übermittlung einzelstaatlicher Dokumente des Geheimhaltungsgrades „TRÈS SECRET UE/EU TOP SECRET“ entspricht;

    c) der Beamte die Dokumente des Geheimhaltungsgrades „TRÈS SECRET UE/EU TOP SECRET“ unter keinen Umständen unbeaufsichtigt lässt;

    d) Vorkehrungen getroffen werden, damit die Liste der Dokumente, die mitgenommen werden, in der „TRÈS SECRET UE/EU TOP SECRET“-Registratur verwahrt, in einem Dienstbuch vermerkt und bei Rückkehr anhand dieses Eintrags kontrolliert wird.

16. Innerhalb ein und desselben Landes dürfen als „SECRET UE“ oder „CONFIDENTIEL UE“ eingestufte Dokumente entweder mit der Post, wenn eine derartige Übermittlung nach den einzelstaatlichen Regelungen gestattet ist und mit den hier vorliegenden Vorschriften in Einklang steht, oder über einen Kurierdienst oder durch Personen übermittelt werden, die zum Zugang zu EU-Verschlusssachen ermächtigt sind.

17. Jeder Mitgliedstaat und jede dezentrale EU-Einrichtung sollte auf diesen Vorschriften beruhende Weisungen für das Personal ausarbeiten, das EU-Verschlusssachen befördert. Es sollte vorgeschrieben werden, dass Personen, die Verschlusssachen befördern, diese Weisungen lesen und

▼B

unterzeichnen. In den Weisungen sollte insbesondere deutlich gemacht werden, dass Dokumente unter keinen Umständen

a) von der sie befördernden Person aus den Händen gegeben werden dürfen, es sei denn, sie seien entsprechend den Bestimmungen in Abschnitt IV in sicherem Gewahrsam;

b) in öffentlichen Transportmitteln oder Privatfahrzeugen oder an Orten wie Restaurants oder Hotels unbeaufsichtigt bleiben dürfen. Sie dürfen nicht in Hotelsafes verwahrt werden oder unbeaufsichtigt in Hotelzimmern zurückbleiben;

c) in der Öffentlichkeit (beispielsweise in Flugzeugen oder Zügen) gelesen werden dürfen.

BEFÖRDERUNG VON EINEM MITGLIEDSTAAT IN EINEN ANDEREN

18. Als „CONFIDENTIEL UE“ oder höher eingestuftes Material sollte durch diplomatische oder militärische Kurierdienste von einem Mitgliedstaat in einen anderen befördert werden.

19. Eine persönliche Beförderung von als „SECRET UE“ oder „CONFIDENTIEL UE“ eingestuftem Material kann jedoch gestattet werden, wenn durch die für die Beförderung geltenden Vorschriften gewährleistet wird, dass das Material nicht in die Hände Unbefugter fallen kann.

20. Die nationalen Sicherheitsbehörden können eine persönliche Beförderung gestatten, wenn keine diplomatischen oder militärischen Kuriere zur Verfügung stehen oder der Rückgriff auf derartige Kuriere zu einer Verzögerung führen würde, die sich nachteilig auf Maßnahmen der EU auswirken könnte, und wenn das Material vom Empfänger dringend benötigt wird. Jeder Mitgliedstaat sollte Anweisungen über die zwischenstaatliche persönliche Beförderung von Material des Geheimhaltungsgrades „SECRET UE“ oder geringer durch Personen, die keine diplomatischen oder militärischen Kuriere sind, ausarbeiten. In diesen Anweisungen sollte vorgesehen werden, dass

a) die Person, die das Material mit sich führt, über die entsprechende, von den Mitgliedstaaten ausgesprochene Zugangsermächtigung verfügen muss;

b) sämtliches auf diese Weise beförderte Material im zuständigen Amt oder der zuständigen Registratur verzeichnet sein muss;

c) Versandstücke oder Taschen, die EU-Material enthalten, mit einem Dienstsiegel zu versehen sind, um Zollkontrollen zu vermeiden oder diesen vorzubeugen, sowie mit Etiketten zu ihrer Erkennung und mit Weisungen für den Finder;

d) die Person, die das Material mit sich führt, einen Kurierausweis und/oder einen Dienstreiseauftrag mitführen muss, die von allen EU-Mitgliedstaaten anerkannt sind und ihn ermächtigen, das betreffende Versandstück in der beschriebenen Weise zu befördern;

e) bei Überlandreisen die Grenze keines Staates, der nicht EU-Mitglied ist, überschritten oder dieser Staat durchfahren werden darf, es sei denn, dass der Staat, der die Beförderung vornimmt, über eine besondere Garantie seitens dieses Staats verfügt;

f) die Reiseplanung der Person, die das Material mit sich führt, im Hinblick auf Bestimmungsorte, Fahrtrouten und Beförderungsmittel mit den EU-Vorschriften oder mit einzelstaatlichen Vorschriften, falls diese in dieser Hinsicht strenger sind, in Einklang stehen muss;

g) das Material von der Person, die es mit sich führt, nicht aus der Hand gegeben werden darf, außer wenn es nach den Bestimmungen des Abschnitts IV über sicheren Gewahrsam verwahrt ist;

h) das Material nicht in öffentlichen Transportmitteln oder Privatfahrzeugen oder an Orten wie Restaurants oder Hotels unbeaufsichtigt bleiben darf. Es darf nicht in Hotelsafes verwahrt werden oder unbeaufsichtigt in Hotelzimmern zurückbleiben;

i) Dokumente, falls solche Bestandteil des beförderten Materials sind, nicht in der Öffentlichkeit (beispielsweise in Flugzeugen, Zügen usw.) gelesen werden dürfen.

Die mit der Beförderung der Verschlusssachen beauftragte Person muss Geheimschutzvorschriften lesen und unterzeichnen, die mindestens die vorstehenden Weisungen sowie Verfahren enthalten, die im Notfall oder für den Fall zu beachten sind, dass das Versandstück mit den Verschlusssachen von Zollbeamten oder Sicherheitsbeamten auf einem Flughafen kontrolliert werden soll.

▼B

ÜBERMITTLUNG VON DOKUMENTEN DES GEHEIMHALTUNGSGRADES „RESTREINT UE“

21. Für die Beförderung von als „RESTREINT UE“ eingestuften Dokumenten werden keine besonderen Vorschriften eingeführt; bei ihrer Beförderung ist allerdings sicherzustellen, dass sie nicht in die Hände Unbefugter geraten können.

SICHERHEIT DER KURIERE

22. Alle Kuriere und Boten, die mit der Beförderung von „SECRET UE“- und „CONFIDENTIEL UE“-Dokumenten beauftragt werden, müssen entsprechend sicherheitsermächtigt sein.

Kapitel III

Elektronische und andere technische Übermittlungswege

23. Mit den Maßnahmen für die Kommunikationssicherheit soll die sichere Übermittlung von EU-Verschlusssachen gewährleistet werden. Die für die Übermittlung dieser EU-Verschlusssachen geltenden Vorschriften sind in Abschnitt XI dargelegt.

24. Als „CONFIDENTIEL UE“ oder „SECRET UE“ eingestufte Informationen dürfen nur von zugelassenen Kommunikationszentren und -netzen und/oder Terminals bzw. über entsprechende Systeme übermittelt werden.

Kapitel IV

Zusätzliche Kopien und Übersetzungen von beziehungsweise Auszüge aus EU-Verschlusssachen

25. Das Kopieren oder die Übersetzung von „TRÈS SECRET UE/EU TOP SECRET“-Dokumenten kann ausschließlich der Urheber gestatten.

26. Fordern Personen, die nicht über eine „TRÈS SECRET UE/EU TOP SECRET“-Sicherheitsermächtigung verfügen, Informationen an, die zwar in einem „TRÈS SECRET UE/EU TOP SECRET“-Dokument enthalten, aber nicht als solche eingestuft sind, so kann der Leiter der „TRÈS SECRET UE/EU TOP SECRET“-Registratur ermächtigt werden, die notwendige Anzahl von Auszügen aus diesem Dokument auszuhändigen. Gleichzeitig ergreift er die erforderlichen Maßnahmen, um sicherzustellen, dass diese Auszüge einen angemessenen Geheimhaltungsgrad erhalten.

27. Als „SECRET UE“ und niedriger eingestufte Dokumente können vom Empfänger unter Einhaltung der einzelstaatlichen Sicherheitsvorschriften und unter strikter Befolgung des Grundsatzes „Kenntnis nur wenn nötig“ vervielfältigt und übersetzt werden. Die für das Originaldokument geltenden Sicherheitsvorschriften finden auch auf Vervielfältigungen und/oder Übersetzungen dieses Dokuments Anwendung. Dezentrale EU-Einrichtungen halten sich an diese Sicherheitsvorschriften.

Kapitel V

Bestandsaufnahme, Prüfung, Archivierung und Vernichtung von EU-Verschlusssachen

BESTANDSAUFNAHME UND PRÜFUNG

28. Alljährlich führt jede „TRÈS SECRET UE/EU TOP SECRET“-Registratur im Sinne des Abschnitts VIII gemäß den Vorschriften des Abschnitts VIII Nummern 9 bis 11 eine detaillierte Bestandsaufnahme der „TRÈS SECRET UE/EU TOP SECRET“-Dokumente durch. EU-Verschlusssachen unterhalb des Geheimhaltungsgrades „TRÈS SECRET UE/EU TOP SECRET“ werden gemäß den einzelstaatlichen Leitlinien oder im Falle des Generalsekretariats des Rates oder dezentraler EU-Einrichtungen gemäß den Anweisungen des Generalsekretärs/Hohen Vertreters einer internen Prüfung unterzogen.

Hierbei soll ermittelt werden, ob nach Auffassung der Verwahrer

a) bestimmte Dokumente heruntergestuft oder der Geheimhaltungsgrad aufgehoben werden kann,

b) Dokumente vernichtet werden sollten.

ARCHIVIERUNG VON EU-VERSCHLUSSSACHEN

29. Um Archivierungsprobleme möglichst gering zu halten, ist es den Kontrollbeamten aller Registraturen gestattet, „TRÈS SECRET UE/EU TOP SECRET“-, „SECRET UE“- und „CONFIDENTIEL UE“-Dokumente auf

▼B

Mikrofilm aufzunehmen oder auf andere Weise auf magnetischen oder optischen Datenträgern zu Archivzwecken zu speichern, vorausgesetzt

a) das Mikrofilm-Speicherverfahren wird von Personen durchgeführt, die über eine Sicherheitsermächtigung für den dem Dokument entsprechenden Geheimhaltungsgrad verfügen;

b) für den Mikrofilm/Datenträger wird die gleiche Sicherheit gewährleistet wie für die Originaldokumente;

c) das Mikrofilmen/die Speicherung eines „TRÈS SECRET UE/EU TOP SECRET"-Dokuments wird dem Urheber mitgeteilt;

d) die Filmrollen oder sonstigen Träger enthalten nur Dokumente der gleichen „TRÈS SECRET UE/EU TOP SECRET"-, „SECRET UE"- oder „CONFIDENTIEL UE"-Einstufung;

e) das Mikrofilmen/die Speicherung eines „TRÈS SECRET UE/EU TOP SECRET"- oder „SECRET UE"-Dokuments wird in dem für die jährliche Bestandsaufnahme verwendeten Register deutlich kenntlich gemacht;

f) die Originaldokumente, die auf Mikrofilm aufgenommen oder in anderer Weise gespeichert sind, werden gemäß den Vorschriften der Nummern 31 bis 36 vernichtet.

30. Diese Vorschriften gelten auch für alle anderen, von der Nationalen Sicherheitsbehörde zugelassenen Speichermedien wie elektromagnetische Träger und optische Speicherplatten.

ROUTINEMÄSSIGE VERNICHTUNG VON EU-VERSCHLUSSSACHEN

31. Um eine unnötige Anhäufung von EU-Verschlusssachen zu vermeiden, werden die nach Auffassung des Leiters der aufbewahrenden Stelle inhaltlich überholten oder überzähligen Dokumente so bald wie praktisch möglich auf folgende Weise vernichtet:

a) „TRÈS SECRET UE/EU TOP SECRET"-Dokumente werden nur von der für diese Dokumente zuständigen Zentralregistratur vernichtet. Jedes der Vernichtung zugeführte Dokument wird auf einer Vernichtungsbescheinigung eingetragen, die vom „TRÈS SECRET UE/EU TOP SECRET"-Kontrollbeamten und von dem der Vernichtung als Zeuge beiwohnenden Beamten, der über die betreffende Sicherheitsermächtigung verfügt, zu unterzeichnen ist. Der Vorgang wird im Dienstbuch festgehalten.

b) Die Registratur bewahrt die Vernichtungsbescheinigungen zusammen mit den Verteilungsunterlagen zehn Jahre lang auf. Dem Urheber oder der zuständigen Zentralregistratur werden Kopien nur zugesandt, wenn dies ausdrücklich verlangt wird.

c) „TRÈS SECRET UE/EU TOP SECRET"-Dokumente einschließlich des bei ihrer Herstellung angefallenen und als Verschlusssache zu behandelnden Abfalls oder Zwischenmaterials wie fehlerhafte Kopien, Arbeitsvorlagen, maschinegeschriebene Aufzeichnungen und Kohlepapier werden unter der Aufsicht eines „TRÈS SECRET UE/EU TOP SECRET"-Beamten durch Verbrennen, Einstampfen, Zerkleinern oder andere geeignete Verfahren so vernichtet, dass der Inhalt weder erkennbar ist noch erkennbar gemacht werden kann.

32. „SECRET UE"-Dokumente werden mittels eines der in Nummer 31 Buchstabe c) genannten Verfahren unter der Aufsicht einer Person, die über die betreffende Sicherheitsermächtigung verfügt, von der für diese Dokumente zuständigen Registratur vernichtet. Vernichtete „SECRET UE"-Dokumente werden auf einer unterzeichneten Vernichtungsbescheinigung eingetragen, die von der Registratur zusammen mit den Verteilungsunterlagen mindestens drei Jahre lang aufbewahrt wird.

33. „CONFIDENTIEL UE"-Dokumente werden mittels eines der in Nummer 31 Buchstabe c) genannten Verfahren unter der Aufsicht einer Person, die über die betreffende Sicherheitsermächtigung verfügt, von der für diese Dokumente zuständigen Registratur vernichtet. Ihre Vernichtung wird gemäß den einzelstaatlichen Vorschriften oder, im Falle des Generalsekretariats des Rates oder dezentraler EU-Einrichtungen, gemäß den Anweisungen des Generalsekretärs/Hohen Vertreters registriert.

34. „RESTREINT UE"-Dokumente werden von der für diese Dokumente zuständigen Registratur gemäß den einzelstaatlichen Vorschriften oder, im Falle des Generalsekretariats des Rates oder dezentraler EU-Einrichtungen, gemäß den Anweisungen des Generalsekretärs/Hohen Vertreters vernichtet.

VERNICHTUNG IM NOTFALL

35. Das Generalsekretariat des Rates, die Mitgliedstaaten und die dezentralen EU-Einrichtungen arbeiten unter Berücksichtigung der örtlichen Gegeben-

▼B

heiten Pläne zum Schutz von EU-Verschlusssachen im Krisenfall aus, die, falls erforderlich, auch Pläne für eine Vernichtung oder Auslagerung der EU-Verschlusssachen im Notfall umfassen; sie erteilen innerhalb ihrer Organisation die Anweisungen, die sie für notwendig erachten, damit EU-Verschlusssachen nicht in unbefugte Hände gelangen.

36. Regelungen zum Schutz und/oder zur Vernichtung von „SECRET UE"- und „CONFIDENTIEL UE"-Unterlagen im Krisenfall dürfen auf keinen Fall den Schutz oder die Vernichtung von „TRÈS SECRET UE/EU TOP SECRET"-Materialien, einschließlich der Verschlüsselungseinrichtungen, beeinträchtigen, die Vorrang vor allen anderen Aufgaben haben. Die für den Schutz und die Vernichtung der Verschlüsselungseinrichtungen vorzusehenden Maßnahmen sind durch Ad-hoc-Anweisungen zu regeln.

Kapitel VI

Spezielle Vorschriften für Dokumente, die für den Rat bestimmt sind

37. Innerhalb des Generalsekretariats des Rates verfolgt ein „Verschlusssachenbüro" die Behandlung der als „SECRET UE" und „CONFIDENTIEL UE" eingestuften Informationen, wenn sie Gegenstand von Ratsdokumenten sind.

Unter der Verantwortung des Generaldirektors für Personal und Verwaltung nimmt es folgende Aufgaben wahr:

a) Verwaltung der Registrierung, Vervielfältigung, Übersetzung, Weiterleitung, Versendung und Vernichtung der Informationen;

b) Führung des Verschlusssachenregisters;

c) regelmäßige Anfragen bei den Urhebern, ob die Einstufung der betreffenden Informationen aufrechtzuerhalten ist;

d) im Benehmen mit dem Sicherheitsdienst Festlegung des praktischen Vorgehens bei der Einstufung und der Aufhebung des Geheimhaltungsgrades von Informationen.

38. Das Verschlusssachenbüro führt ein Register mit folgenden Angaben:

a) Datum der Erstellung der Verschlusssache,

b) Geheimhaltungsgrad,

c) Sperrfrist,

d) Name und Dienststelle des Urhebers,

e) der oder die Empfänger mit laufender Nummer,

f) Gegenstand,

g) Nummer,

h) Zahl der verbreiteten Exemplare,

i) Erstellung von Bestandsverzeichnissen der dem Rat unterbreiteten Verschlusssachen,

j) Register betreffend die Aufhebung des Geheimhaltungsgrades und die Herabstufung von Verschlusssachen.

39. Für das Verschlusssachenbüro des Generalsekretariats des Rates gelten die allgemeinen Vorschriften der Kapitel I bis V dieses Abschnitts, soweit sie nicht durch die spezifischen Vorschriften dieses Kapitels geändert werden.

▼B

ABSCHNITT VIII

„TRÈS SECRET UE/EU TOP SECRET“-REGISTRATUREN

1. Durch „TRÈS SECRET UE/EU TOP SECRET“-Registraturen ist zu gewährleisten, dass die Registrierung, Handhabung und Verteilung von „TRÈS SECRET UE/EU TOP SECRET“-Dokumenten gemäß den Sicherheitsvorschriften erfolgt. Die Leiter der „TRÈS SECRET UE/EU TOP SECRET“-Registraturen in den einzelnen Mitgliedstaaten, beim Generalsekretariat des Rates und gegebenenfalls in dezentralen EU-Einrichtungen sind „TRÈS SECRET UE/EU TOP SECRET“-Kontrollbeamte.

2. Die Zentralregistraturen sind die hauptsächliche Empfangs- und Versandbehörde in den Mitgliedstaaten, beim Generalsekretariat des Rates und in dezentralen EU-Einrichtungen, in denen solche Registraturen eingerichtet wurden, sowie gegebenenfalls in anderen EU-Einrichtungen, internationalen Organisationen und Drittstaaten, mit denen der Rat Abkommen über die Sicherheitsverfahren für den Austausch von Verschlusssachen geschlossen hat.

3. Nötigenfalls werden Unterregistraturen eingerichtet, die für die interne Verwaltung von „TRÈS SECRET UE/EU TOP SECRET“-Dokumenten zuständig sind; sie führen ein Register der von ihnen aufbewahrten Dokumente, das stets auf dem neuesten Stand gehalten wird.

4. „TRÈS SECRET UE/EU TOP SECRET“-Unterregistraturen werden nach Maßgabe des Abschnitts I eingerichtet, damit längerfristigen Notwendigkeiten entsprochen werden kann; sie werden einer zentralen „TRÈS SECRET UE/EU TOP SECRET“-Registratur zugeordnet. Müssen „TRÈS SECRET UE/EU TOP SECRET“-Dokumente nur zeitweilig und gelegentlich konsultiert werden, so können sie ohne Einrichtung einer „TRÈS SECRET UE/EU TOP SECRET“-Unterregistratur weitergeleitet werden, sofern Vorschriften festgelegt wurden, die gewährleisten, dass diese Dokumente unter der Kontrolle der entsprechenden „TRÈS SECRET UE/EU TOP SECRET“-Registratur verbleiben und alle materiellen und personenbezogenen Sicherheitsmaßnahmen eingehalten werden.

5. Unterregistraturen ist es nicht gestattet, ohne ausdrückliche Zustimmung ihrer „TRÈS SECRET UE/EU TOP SECRET“-Zentralregistratur „TRÈS SECRET UE/EU TOP SECRET“-Dokumente unmittelbar an andere Unterregistraturen derselben Zentralregistratur zu übermitteln.

6. Der Austausch von „TRÈS SECRET UE/EU TOP SECRET“-Dokumenten zwischen Unterregistraturen, die nicht derselben Zentralregistratur zugeordnet sind, muss über die „TRÈS SECRET UE/EU TOP SECRET“-Zentralregistraturen abgewickelt werden.

„TRÈS SECRET UE/EU TOP SECRET“-ZENTRALREGISTRATUREN

7. In seiner Eigenschaft als Kontrollbeamter ist der Leiter einer „TRÈS SECRET UE/EU TOP SECRET“-Zentralregistratur zuständig für

   a) die Übermittlung von „TRÈS SECRET UE/EU TOP SECRET“-Dokumenten gemäß den in Abschnitt VII festgelegten Vorschriften;

   b) die Führung einer Liste aller ihm unterstehenden „TRÈS SECRET UE/EU TOP SECRET“-Unterregistraturen mit Name und Unterschrift der ernannten Kontrollbeamten und ihrer bevollmächtigten Stellvertreter;

   c) die Aufbewahrung der Empfangsbescheinigungen der Registraturen für alle von der Zentralregistratur verteilten „TRÈS SECRET UE/EU TOP SECRET“-Dokumente;

   d) die Führung eines Registers aller aufbewahrten und verteilten „TRÈS SECRET UE/EU TOP SECRET“-Dokumente;

   e) die Führung einer aktuellen Liste aller „TRÈS SECRET UE/EU TOP SECRET“-Zentralregistraturen, mit denen er üblicherweise korrespondiert, mit Name und Unterschrift der ernannten Kontrollbeamten und ihrer bevollmächtigten Stellvertreter;

   f) den materiellen Schutz aller in der Registratur aufbewahrten „TRÈS SECRET UE/EU TOP SECRET“-Dokumente gemäß den Vorschriften des Abschnitts IV.

„TRÈS SECRET UE/EU TOP SECRET“-UNTERREGISTRATUREN

8. In seiner Eigenschaft als Kontrollbeamter ist der Leiter einer „TRÈS SECRET UE/EU TOP SECRET“-Unterregistratur zuständig für

   a) die Übermittlung von „TRÈS SECRET UE/EU TOP SECRET“-Dokumenten gemäß den in Abschnitt VII und Abschnitt VIII Nummern 5 und 6 festgelegten Vorschriften;

▼B

b) die Führung einer aktuellen Liste aller Personen, die befugt sind, Zugang zu den „TRÈS SECRET UE/EU TOP SECRET“-Informationen zu erhalten, welche seiner Aufsicht unterliegen;

c) die Verteilung von „TRÈS SECRET UE/EU TOP SECRET“-Dokumenten gemäß den Vorschriften des Herausgebers oder nach dem Grundsatz „Kenntnis nur wenn nötig“, nach vorheriger Prüfung, ob der Empfänger die erforderliche Sicherheitsermächtigung erhalten hat;

d) die Führung eines auf neuestem Stand zu haltenden Registers aller aufbewahrten oder in Umlauf befindlichen „TRÈS SECRET UE/EU TOP SECRET“-Dokumente, die seiner Aufsicht unterliegen oder die an andere „TRÈS SECRET UE/EU TOP SECRET“-Registraturen weitergeleitet wurden, und Aufbewahrung aller entsprechenden Empfangsbescheinigungen;

e) die Führung einer aktuellen Liste der „TRÈS SECRET UE/EU TOP SECRET“-Registraturen, mit denen er „TRÈS SECRET UE/EU TOP SECRET“-Dokumente austauschen darf, mit Name und Unterschrift ihrer ernannten Kontrollbeamten und bevollmächtigten Stellvertreter;

f) den materiellen Schutz aller in der Unterregistratur aufbewahrten „TRÈS SECRET UE/EU TOP SECRET“ Dokumente gemäß den Vorschriften des Abschnitts IV.

BESTANDSAUFNAHMEN

9. Alle zwölf Monate führt jede „TRÈS SECRET UE/EU TOP SECRET“-Registratur eine ausführliche Bestandsaufnahme aller „TRÈS SECRET UE/EU TOP SECRET“-Dokumente durch, für die sie nachweispflichtig ist. Als nachgewiesen gilt jedes Dokument, das in der Registratur materiell vorhanden ist oder für das die Empfangsbescheinigung einer „TRÈS SECRET UE/EU TOP SECRET“-Registratur, der das Dokument übermittelt wurde, bzw. eine Vernichtungsbescheinigung oder aber eine Anweisung zur Herabstufung dieses Dokuments oder der Aufhebung seines Geheimhaltungsgrades vorliegt.

10. Die Unterregistraturen übermitteln die Ergebnisse ihrer jährlichen Bestandsaufnahme der Zentralregistratur, der sie unterstehen, zu einem von dieser festgelegten Datum.

11. Die nationalen Sicherheitsbehörden und die EU-Einrichtungen, die internationalen Organisationen und die dezentralen EU-Einrichtungen, in denen eine „TRÈS SECRET UE/EU TOP SECRET“-Zentralregistratur eingerichtet wurde, übermitteln dem Generalsekretär/Hohen Vertreter spätestens zum 1. April eines jeden Jahres die Ergebnisse der jährlichen Bestandsaufnahme ihrer „TRÈS SECRET UE/EU TOP SECRET“-Zentralregistraturen.

▼B

ABSCHNITT IX

SICHERHEITSMASSNAHMEN BEI BESONDEREN TAGUNGEN AUSSERHALB DER RATSGEBÄUDE, BEI DENEN HOCH EMPFINDLICHE ANGELEGENHEITEN ERÖRTERT WERDEN

ALLGEMEINES

1. Finden Tagungen des Europäischen Rates, Rats- und Ministertagungen oder andere wichtige Tagungen außerhalb der in Brüssel und Luxemburg befindlichen Gebäude des Rates statt und ist es durch die besonderen Sicherheitsanforderungen aufgrund der hohen Empfindlichkeit der behandelten Fragen oder Informationen gerechtfertigt, so werden die nachstehend beschriebenen Sicherheitsmaßnahmen ergriffen. Diese Maßnahmen betreffen lediglich den Schutz von EU-Verschlusssachen; möglicherweise sind weitere Sicherheitsmaßnahmen vorzusehen.

VERANTWORTLICHKEITEN

Gastgebender Mitgliedstaat

2. Der Mitgliedstaat, in dessen Gebiet eine Tagung des Europäischen Rates, eine Rats- oder Ministertagung oder eine andere wichtige Tagung stattfindet (gastgebender Mitgliedstaat), sollte in Zusammenarbeit mit dem Sicherheitsbüro des Generalsekretariats des Rates für die Sicherheit dieser Tagung und die materielle Sicherheit der Hauptdelegierten und ihres Personals verantwortlich sein.

   In Bezug auf den Sicherheitsschutz sollte der Mitgliedstaat insbesondere gewährleisten, dass

   a) Pläne für den Umgang mit Sicherheitsrisiken und sicherheitsrelevanten Zwischenfällen aufgestellt werden, wobei die betreffenden Maßnahmen insbesondere auf die sichere Verwahrung von EU-Verschlusssachen in Büroräumen abzielen;

   b) Maßnahmen getroffen werden, um den etwaigen Zugang zum Kommunikationssystem des Rates für den Empfang und die Versendung von eingestuften EU-Nachrichten bereitzustellen. Der gastgebende Mitgliedstaat wird erforderlichenfalls ferner den Zugang zu sicheren Telefonsystemen bereitstellen.

Mitgliedstaaten

3. Die Behörden der Mitgliedstaaten sollten die erforderlichen Maßnahmen treffen, um dafür zu sorgen, dass

   a) für ihre nationalen Delegierten geeignete Sicherheitsunbedenklichkeitsbescheinigungen bereitgestellt und erforderlichenfalls per Signalübertragung oder Fax entweder unmittelbar oder über das Sicherheitsbüro des Generalsekretariats des Rates dem Sicherheitsbeauftragten für die betreffende Tagung übermittelt werden;

   b) alle besonderen Risiken den Behörden des gastgebenden Mitgliedstaats und erforderlichenfalls dem Sicherheitsbüro des Generalsekretariats des Rates mitgeteilt werden, so dass geeignete Abhilfemaßnahmen getroffen werden können.

Sicherheitsbeauftragter für die Tagung

4. Es sollte ein Sicherheitsbeauftragter ernannt werden, der für die allgemeine Vorbereitung und Überwachung der allgemeinen internen Sicherheitsmaßnahmen und für die Koordinierung mit den anderen betroffenen Sicherheitsbehörden verantwortlich ist. Die vom ihm getroffenen Maßnahmen sollten sich im Allgemeinen auf Folgendes erstrecken:

   a) i) Schutzmaßnahmen am Tagungsort, mit denen sichergestellt wird, dass es auf der Tagung zu keinem Zwischenfall kommt, der die Sicherheit einer dort verwendeten EU-Verschlusssache gefährden könnte;

      ii) Überprüfung des Personals, das den Tagungsort, die Bereiche der Delegationen und die Konferenzräume betreten darf, sowie sämtlicher Ausrüstungsgegenstände;

      iii) ständige Abstimmung mit den zuständigen Behörden des gastgebenden Mitgliedstaats und dem Sicherheitsbüro des Generalsekretariats des Rates;

   b) Einfügung von Sicherheitsanweisungen in das Tagungsdossier unter gebührender Berücksichtigung der Erfordernisse, die in diesen Sicherheitsvorschriften und anderen für erforderlich erachteten Sicherheitsanweisungen enthalten sind.

▼B

Sicherheitsbüro des Generalsekretariats des Rates

5. Das Sicherheitsbüro des Generalsekretariats des Rates sollte als Sicherheitsberatungsstelle für die Vorbereitung der Tagung fungieren; es sollte auf der Tagung vertreten sein, um erforderlichenfalls den Sicherheitsbeauftragten für die Tagung und die Delegationen zu unterstützen und zu beraten.

6. Jede an der Tagung teilnehmende Delegation sollte einen Sicherheitsbeauftragten benennen, der für die Behandlung von Sicherheitsfragen in seiner Delegation zuständig ist und die Verbindung zu dem Sicherheitsbeauftragten für die Tagung sowie mit dem Vertreter des Sicherheitsbüros des Generalsekretariats des Rates aufrecht erhält.

SICHERHEITSMASSNAHMEN

Sicherheitsbereiche

7. Es werden folgende Sicherheitsbereiche angelegt:

   a) ein Sicherheitsbereich der Kategorie II, der nach Maßgabe der Erfordernisse einen Redaktionsraum, die Büroräume des Generalsekretariats des Rates und die Vervielfältigungsausrüstung sowie die Büroräume der Delegationen umfasst;

   b) ein Sicherheitsbereich der Kategorie I, der den Konferenzraum sowie die Dolmetschkabinen und die Kabinen für die Tontechnik umfasst;

   c) einen Verwaltungsbereich, der aus dem Pressebereich und den für Verwaltung, Verpflegung und Unterkunft genutzten Bereichen des Tagungsorts sowie aus dem sich unmittelbar an das Pressezentrum und den Tagungsort anschließenden Bereich besteht.

Berechtigungsausweise

8. Der Sicherheitsbeauftragte für die Tagung sollte entsprechend den von den Delegationen gemeldeten Bedarf geeignete Berechtigungsausweise ausgeben. Erforderlichenfalls kann eine Abstufung der Zugangsberechtigung für die verschiedenen Sicherheitsbereiche vorgesehen werden.

9. Mit den Sicherheitsanweisungen für die Tagung sollten alle Betroffenen verpflichtet werden, am Tagungsort ihre Berechtigungsausweise stets gut sichtbar mit sich zu führen, so dass sie erforderlichenfalls vom Sicherheitspersonal überprüft werden können.

10. Abgesehen von den mit einem Berechtigungsausweis versehenen Tagungsteilnehmern sollten so wenige Personen wie möglich Zugang zum Tagungsort erhalten. Die einzelstaatlichen Delegationen, die während der Tagung Besucher empfangen möchten, sollten dies dem Sicherheitsbeauftragten für die Tagung mitteilen. Die Besucher sollten einen Besucherausweis erhalten. Es sollte ein Besuchsnachweisformblatt ausgefüllt werden, in das der Name des Besuchers und der Name der besuchten Person eingetragen werden. Besucher sollten stets von einem Angehörigen des Sicherheitspersonals oder von der besuchten Person begleitet werden. Das Besuchsnachweisformblatt sollte von der begleitenden Person mitgeführt und von dieser zusammen mit dem Besucherausweis dem Sicherheitspersonal zurückgegeben werden, sobald der Besucher den Tagungsort verlässt.

Kontrolle von fotografischen Ausrüstungen und Tonaufzeichnungsgeräten

11. Bild- oder Tonaufzeichnungsgeräte dürfen nicht in einen Sicherheitsbereich der Kategorie I gebracht werden, sofern es sich nicht um die Ausrüstung von Fotografen und Tontechnikern handelt, die vom Sicherheitsbeauftragten der Tagung vorschriftsgemäß zugelassen worden sind.

Überprüfung von Aktentaschen, tragbaren Computern und Paketen

12. Inhaber von Berechtigungsausweisen, denen der Zugang zu einem Sicherheitsbereich gestattet ist, dürfen für gewöhnlich ihre Aktentaschen und tragbaren Computer (nur mit eigener Stromversorgung) mitbringen, ohne dass diese überprüft werden. Bei für die Delegationen bestimmten Paketen dürfen die Delegationen die Lieferung in Empfang nehmen; diese wird entweder vom Sicherheitsbeauftragten der Delegation überprüft und mit Spezialgeräten kontrolliert oder aber vom Sicherheitspersonal zur Überprüfung geöffnet. Wenn der Sicherheitsbeauftragte für die Tagung es für erforderlich hält, können strengere Maßnahmen für die Überprüfung von Aktentaschen und Paketen festgelegt werden.

Technische Sicherheit

13. Der Tagungsraum kann von einem für die technische Sicherheit zuständigen Team technisch gesichert werden; dieses Team kann ferner während der Tagung eine elektronische Überwachung vornehmen.

▼B

Dokumente der Delegationen

14. Die Delegationen sollten für die Beförderung von EU-Verschlusssachen zu und von Tagungen verantwortlich sein. Sie sollten auch für die Überprüfung und Sicherheit der betreffenden Unterlagen bei der Verwendung in den ihnen zugewiesenen Räumlichkeiten verantwortlich sein. Der gastgebende Mitgliedstaat kann für die Beförderung der Verschlusssachen zum und vom Tagungsort um Hilfe ersucht werden.

Sichere Aufbewahrung der Dokumente

15. Sind das Generalsekretariat des Rates, die Kommission oder die Delegationen nicht in der Lage, ihre Verschlusssachen gemäß den anerkannten Standards aufzubewahren, so können sie diese Unterlagen in einem versiegelten Umschlag beim Sicherheitsbeauftragten für die Tagung gegen Empfangsbescheinigung hinterlegen, so dass dieser für eine den genannten Standards entsprechenden Aufbewahrung Sorge tragen kann.

Überprüfung der Büroräume

16. Der Sicherheitsbeauftragte der Tagung sollte dafür sorgen, dass die Büroräume des Generalsekretariats des Rates und der Delegationen am Ende jedes Arbeitstages überprüft werden, damit sichergestellt ist, dass alle EU-Verschlusssachen an einem sicheren Ort aufbewahrt werden; andernfalls sollte er die erforderlichen Abhilfemaßnahmen treffen.

Abfallbeseitigung bei EU-Verschlusssachen

17. Sämtliche Abfälle sind als EU-Verschlusssachen zu behandeln und das Generalsekretariat des Rates und die Delegationen sollten zur Entsorgung Papierkörbe oder Abfallsäcke erhalten. Das Generalsekretariat des Rates und die Delegationen sollten vor Verlassen der ihnen zugewiesenen Räumlichkeiten die Abfälle zum Sicherheitsbeauftragten für die Tagung bringen, der ihre vorschriftsmäßige Vernichtung veranlasst.

18. Am Ende der Tagung sollten alle Dokumente, die das Generalsekretariat des Rates oder die Delegationen in ihrem Besitz hatten, aber nicht behalten wollen, als Abfall behandelt werden. Es sollte eine umfassende Inspektion der Räumlichkeiten des Generalsekretariats des Rates und der Delegationen durchgeführt werden, bevor die für die Tagung getroffenen Sicherheitsmaßnahmen aufgehoben werden. Dokumente, für die eine Empfangsbescheinigung unterzeichnet wurde, sollten soweit möglich gemäß den Vorschriften des Abschnitts VII vernichtet werden.

▼B

ABSCHNITT X

VERLETZUNG DER SICHERHEIT UND KENNTNISNAHME VON EU-VERSCHLUSSSACHEN DURCH UNBEFUGTE

1. Zu einer Verletzung der Sicherheit kommt es, wenn durch eine Handlung oder durch eine Unterlassung, die den Sicherheitsvorschriften des Rates oder eines der Mitgliedstaaten zuwiderläuft, EU-Verschlusssachen in Gefahr geraten oder Unbefugten zur Kenntnis gelangen.

2. Eine Kenntnisnahme von EU-Verschlusssachen durch Unbefugte liegt vor, wenn die Verschlusssachen ganz oder teilweise in die Hände unbefugter Personen (d. h. von Personen, die nicht die erforderliche Zugangsermächtigung haben oder deren Kenntnis der Verschlusssachen nicht nötig ist) gelangt sind oder es wahrscheinlich ist, dass eine derartige Kenntnisnahme stattgefunden hat.

3. Die Kenntnisnahme von EU-Verschlusssachen durch Unbefugte kann die Folge von Nachlässigkeit, Fahrlässigkeit oder Indiskretion, aber auch der Tätigkeit von Diensten, die in der EU oder ihren Mitgliedstaaten Kenntnis von EU-Verschlusssachen und geheimen Tätigkeiten erlangen wollen, oder von subversiven Organisationen sein.

4. Es ist wichtig, dass alle Personen, die mit EU-Verschlusssachen umgehen müssen, eingehend über die Sicherheitsverfahren, die Gefahren von indiskreten Gesprächen und über ihre Beziehungen zur Presse unterrichtet werden. Sie sollten sich darüber im Klaren sein, wie wichtig es ist, jede ihnen bekannt werdende Verletzung der Sicherheit sofort der Sicherheitsbehörde des Mitgliedstaats, des Organs oder der Einrichtung, in dem bzw. der sie beschäftigt sind, mitzuteilen.

5. Wenn eine Sicherheitsbehörde eine Verletzung der Sicherheit betreffend EU-Verschlusssachen oder den Verlust bzw. das Verschwinden von als EU-Verschlusssache eingestuftem Material entdeckt oder hiervon unterrichtet wird, trifft sie rasch Maßnahmen, um

   a) den Sachverhalt zu klären;

   b) den entstandenen Schaden zu bewerten und möglichst klein zu halten;

   c) zu verhindern, dass sich ein derartiger Vorfall wiederholt;

   d) die zuständigen Behörden von den Folgen der Verletzung der Sicherheit zu unterrichten.

   In diesem Zusammenhang sind folgende Angaben zu machen:

   i) eine Beschreibung der entsprechenden Verschlusssache unter Angabe ihres Geheimhaltungsgrades, ihres Aktenzeichens und der Ausfertigungsnummer, des Datums, des Urhebers, des Themas und des Umfangs;

   ii) eine kurze Beschreibung der Umstände, unter denen die Verletzung der Sicherheit erfolgt ist, unter Angabe des Datums und des Zeitraums, während dessen die Verschlusssache Unbefugten zur Kenntnis gelangen konnte;

   iii) eine Erklärung darüber, ob der Urheber informiert worden ist.

6. Jede Sicherheitsbehörde hat die Pflicht, unmittelbar nach ihrer Unterrichtung von einer möglichen Verletzung der Sicherheit hierüber nach dem folgenden Verfahren Bericht zu erstatten: Die Unterregistratur für als „TRÈS SECRET UE/EU TOP SECRET“ eingestufte Verschlusssachen meldet den Vorfall über ihre „TRÈS SECRET UE/EU TOP SECRET“-Zentralregistratur dem Sicherheitsbüro des Generalsekretariats des Rates; ist die Kenntnisnahme von EU-Verschlusssachen durch Unbefugte im Zuständigkeitsbereich eines Mitgliedstaates erfolgt, so wird sie über die zuständige nationale Sicherheitsbehörde auf die in Nummer 5 angegebene Weise dem Sicherheitsbüro des Generalsekretariats des Rates gemeldet.

7. Fälle, in denen es um als „RESTREINT UE“ eingestufte Verschlusssachen geht, müssen nur dann gemeldet werden, wenn sie ungewöhnlicher Art sind.

8. Wird der Generalsekretär/Hohe Vertreter von einer Verletzung der Sicherheit unterrichtet, so

   a) unterrichtet er die Behörde, von der die entsprechende Verschlusssache stammt;

   b) bittet er die entsprechenden Sicherheitsbehörden um die Einleitung von Ermittlungen;

   c) koordiniert er die Ermittlungen, falls mehr als eine Sicherheitsbehörde betroffen ist;

▼B

d) lässt er einen Bericht erstellen über die Umstände der Verletzung der Sicherheit, das Datum oder den Zeitraum, an dem bzw. während dessen die Verletzung erfolgt ist und der Verstoß entdeckt wurde; der Bericht umfasst eine detaillierte Beschreibung des Inhalts und des Geheimhaltungsgrades des betreffenden Materials. Es sollte auch berichtet werden, welcher Schaden den Interessen der EU oder eines oder mehrerer ihrer Mitgliedstaaten entstanden ist und welche Maßnahmen ergriffen worden sind, um eine Wiederholung des Vorfalls zu verhindern.

9. Die Stelle, von der die Verschlusssache stammt, unterrichtet die Empfänger des Dokuments und gibt ihnen entsprechende Anweisungen.

10. Gegen jede für die Kenntnisnahme von EU-Verschlusssachen durch Unbefugte verantwortliche Person können disziplinarische Maßnahmen aufgrund der geltenden Vorschriften und Regelungen ergriffen werden. Diese Maßnahmen lassen ein etwaiges gerichtliches Vorgehen unberührt.

▼B

ABSCHNITT XI

SCHUTZ VON INFORMATIONEN IN INFORMATIONSTECHNISCHEN SYSTEMEN UND KOMMUNIKATIONSSYSTEMEN

Inhalt

▼B

Kapitel I

Einleitung

ALLGEMEINES

1. Das Sicherheitskonzept und die Sicherheitsanforderungen, die in diesem Abschnitt beschrieben werden, gelten für alle Kommunikations- und Informationssysteme und -netze (nachstehend als „SYSTEME“ bezeichnet), in denen Informationen des Geheimhaltungsgrades „CONFIDENTIEL UE“ oder höher verarbeitet werden.

2. Auch bei SYSTEMEN, in denen als „RESTREINT UE“ eingestufte Informationen verarbeitet werden, sind Sicherheitsmaßnahmen zum Schutz der Vertraulichkeit dieser Informationen erforderlich. Bei allen SYSTEMEN sind Sicherheitsmaßnahmen zum Schutz der Integrität und der Verfügbarkeit dieser Systeme und der darin enthaltenen Informationen erforderlich. Die auf diese Systeme anzuwendenden Sicherheitsmaßnahmen werden von der dazu vorgesehenen Akkreditierungsstelle für IT-Sicherheit (Security Accreditation Authority, SAA) festgelegt, sie entsprechen dem festgestellten Risiko und stehen mit dem in diesen Sicherheitsbestimmungen dargelegten Konzept im Einklang.

3. Der Schutz von Sensorsystemen, die eingebettete IT-SYSTEME enthalten, wird im allgemeinen Kontext derjenigen Systeme, deren Bestandteil sie sind, unter weitestgehender Anwendung der jeweiligen Bestimmungen dieses Abschnitts festgelegt und spezifiziert.

BEDROHUNGEN UND SCHWACHSTELLEN VON SYSTEMEN

4. Eine Bedrohung kann allgemein als Möglichkeit einer unabsichtlichen oder absichtlichen Beeinträchtigung der Sicherheit definiert werden. Bei SYSTEMEN ist dies mit dem Verlust einer oder mehrerer der Eigenschaften Vertraulichkeit, Integrität und Verfügbarkeit verbunden. Eine Schwachstelle kann als unzureichende oder fehlende Kontrolle definiert werden, die die Bedrohung eines bestimmten Objekts oder Ziels erleichtern oder ermöglichen könnte. Eine Schwachstelle kann durch ein Versäumnis entstehen oder sie kann mit nachlässigen, unvollständigen oder inkonsistenten Kontrollen zusammenhängen; sie kann die Technik, die Verfahrens- oder die Betriebsebene betreffen.

5. EU-Verschlusssachen und sonstige Informationen, die in SYSTEMEN in einer zur raschen Abfrage, Übermittlung und Nutzung konzipierten konzentrierten Form vorliegen, sind in vielerlei Hinsicht gefährdet. So könnten z. B. Unbefugte auf die Informationen zugreifen oder Befugten könnte der Zugriff verweigert werden. Ferner besteht das Risiko einer unerlaubten Verbreitung, einer Verfälschung, Änderung oder Löschung der Informationen. Außerdem sind die komplexen und manchmal empfindlichen Geräte teuer in der Anschaffung, und es ist häufig schwierig, sie rasch zu reparieren oder zu ersetzen. Deshalb stellen diese SYSTEME attraktive Ziele für geheimdienstliche Tätigkeit oder Sabotage dar, insbesondere wenn die Sicherheitsmaßnahmen für unzureichend gehalten werden.

SICHERHEITSMASSNAHMEN

6. Die in diesem Abschnitt festgelegten Sicherheitsmaßnahmen dienen in erster Linie dem Schutz von Informationen vor unerlaubter Preisgabe (Verlust der Vertraulichkeit), sowie dem Schutz vor dem Verlust der Integrität und der Verfügbarkeit von Informationen. Um ein SYSTEM, in dem EU-Verschlusssachen verarbeitet werden, angemessen zu schützen, sind die einschlägigen konventionellen Sicherheitsstandards festzulegen, zu denen geeignete, auf das jeweilige SYSTEM zugeschnittene spezielle Sicherheitsverfahren und -techniken hinzukommen.

7. Um ein sicheres Umfeld für den Betrieb eines SYSTEMS zu schaffen, muss eine ausgewogene Kombination von Sicherheitsmaßnahmen ausgewählt und umgesetzt werden. Diese Maßnahmen betreffen physische Objekte, das Personal, nichttechnische Verfahren sowie Betriebsverfahren für Computer und Kommunikationssysteme.

8. Bei Maßnahmen im Bereich der Computersicherheit (Sicherheitseigenschaften der Hard- und Software) muss der Grundsatz des berechtigen Informationsbedarfs („Need-to-know-Prinzip“) eingehalten werden, und die unerlaubte Preisgabe von Informationen muss verhindert oder aufgedeckt werden. Wie zuverlässig Maßnahmen der Computersicherheit sein müssen, wird bei der Formulierung der Sicherheitsanforderungen festgelegt. Im Rahmen der Akkreditierung wird überprüft, dass eine angemessene Vertrauenswürdigkeit vorhanden ist, um sich auf Maßnahmen der Computersicherheit verlassen zu können.

▼B

AUFSTELLUNG DER SYSTEMSPEZIFISCHEN SICHERHEITSANFORDERUNGEN (SSRS)

9. Für alle SYSTEME, in denen als „CONFIDENTIEL UE“ oder höher eingestufte Informationen verarbeitet werden, ist eine Aufstellung der systemspezifischen Sicherheitsanforderungen (SYSTEM-Specific Security Requirement Statement, SSRS) erforderlich, die von der für den Betrieb des IT-Systems zuständigen Stelle (IT System Operational Authority, ITSOA) gegebenenfalls mit Beiträgen und Unterstützung des Projektpersonals und der INFOSEC-Stelle erstellt und von der SAA genehmigt wird. Eine SSRS ist auch dann erforderlich, wenn die Verfügbarkeit und Integrität von als „RESTREINT UE“ eingestuften Informationen oder von Informationen ohne VS-Einstufung von der SAA als sicherheitskritisch angesehen wird.

10. Die SSRS wird im frühesten Stadium der Konzeption eines Projekts formuliert und parallel zum Projektverlauf weiterentwickelt und verbessert; sie erfüllt unterschiedliche Aufgaben in verschiedenen Stadien des Projekts und des Lebenszyklus des SYSTEMS.

11. Die SSRS wird zwischen der für den Betrieb des IT-Systems zuständigen Stelle und der SAA verbindlich vereinbart und bei der Akkreditierung des Systems zugrunde gelegt.

12. Die SSRS ist eine vollständige und ausführliche Festlegung der einzuhaltenden Sicherheitsgrundsätze und der zu erfüllenden detaillierten Sicherheitsanforderungen. Sie beruht auf dem Sicherheitskonzept und der Risikobewertung des Rates bzw. wird von Faktoren des betrieblichen Umfelds bestimmt, vom niedrigsten Berechtigungsstatus des Personals, dem höchsten Geheimhaltungsgrad der verarbeiteten Informationen, vom jeweiligen Sicherheitsmodus oder den Benutzeranforderungen. Die SSRS ist Bestandteil der Projektdokumentation, die den zuständigen Stellen zur Billigung der technischen, haushaltsbezogenen und sicherheitsrelevanten Aspekte unterbreitet wird. In ihrer endgültigen Fassung ist die SSRS eine vollständige Beschreibung der Voraussetzungen, die gegeben sein müssen, damit ein bestimmtes SYSTEM sicher ist.

SICHERHEITSMODUS

13. Alle SYSTEME, in denen als „CONFIDENTIEL UE“ oder höher eingestufte Informationen verarbeitet werden, werden für den Betrieb in einem einzigen Sicherheitsmodus oder — aufgrund zeitlich unterschiedlicher Anforderungen — in mehreren der folgenden sicherheitsbezogenen Betriebsarten (oder deren einzelstaatlichen Entsprechungen) freigegeben:

    a) „dedicated“,

    b) „system high“,

    c) „multi-level“.

Kapitel II

Begriffsbestimmungen

ZUSÄTZLICHE KENNZEICHNUNGEN

14. Zusätzliche Kennzeichnungen wie z. B. CRYPTO oder eine andere von der EU anerkannte Sonderkennung werden verwendet, wenn zusätzlich zu der Behandlung, die sich durch die VS-Einstufung ergibt, eine begrenzte Verteilung und eine besondere Abwicklung erforderlich sind.

15. Der SICHERHEITSMODUS „DEDICATED“ bezeichnet eine Betriebsart, bei der ALLE Personen, die Zugang zum SYSTEM haben, zum Zugriff auf den höchsten im SYSTEM verarbeiteten Geheimhaltungsgrad berechtigt sind und generell einen berechtigten Informationsbedarf in Bezug auf ALLE im SYSTEM verarbeiteten Informationen haben.

    Anmerkungen:

    1. Da alle Nutzer einen berechtigten Informationsbedarf haben, muss sicherheitstechnisch nicht unbedingt zwischen unterschiedlichen Informationen innerhalb des SYSTEMS unterschieden werden.

    2. Andere Sicherheitseigenschaften (z. B. objekt-, personen- und verfahrensbezogene Funktionen) müssen den Anforderungen für den höchsten Geheimhaltungsgrad und für alle Kategorien von Informationen, die im SYSTEM verarbeitet werden, entsprechen.

16. Der SICHERHEITSMODUS „SYSTEM-HIGH“ bezeichnet eine Betriebsart, bei der ALLE Personen, die Zugang zum SYSTEM haben, zum Zugriff auf den höchsten im SYSTEM verarbeiteten Geheimhaltungs-

▼B

grad berechtigt sind, bei der aber NICHT ALLE Personen, die Zugang zum System haben, generell einen berechtigten Informationsbedarf in Bezug auf die im SYSTEM verarbeiteten Informationen haben.

Anmerkungen:

1. Da nicht alle Nutzer generell einen berechtigten Informationsbedarf haben, muss die sicherheitstechnische Ausgestaltung einen selektiven Zugriff auf Informationen und eine Trennung von Informationen innerhalb des SYSTEMS gewährleisten.

2. Andere Sicherheitseigenschaften (z. B. objekt-, personen- und verfahrensbezogene Funktionen) müssen den Anforderungen für den höchsten Geheimhaltungsgrad und für alle Kategorien von Informationen, die im SYSTEM verarbeitet werden, entsprechen.

3. Bei dieser Betriebsart werden alle im SYSTEM verarbeiteten oder für das SYSTEM verfügbaren Informationen sowie die entsprechenden Ausgaben — solange nichts anderes festgelegt wurde — so geschützt, als würden sie unter die jeweilige Kategorie von Informationen und den höchsten verarbeiteten Geheimhaltungsgrad fallen, es sei denn, eine vorhandene Kennzeichnungsfunktion ist in ausreichendem Maße vertrauenswürdig.

17. Der SICHERHEITSMODUS „MULTI-LEVEL“ bezeichnet eine Betriebsart, bei der NICHT ALLE Personen, die Zugang zum SYSTEM haben, zum Zugriff auf den höchsten Geheimhaltungsgrad im SYSTEM berechtigt sind und bei der NICHT ALLE Personen, die Zugang zum System haben, generell einen berechtigten Informationsbedarf in Bezug auf die im SYSTEM verarbeiteten Informationen haben.

Anmerkungen:

1. In dieser Betriebsart ist derzeit die Verarbeitung von Informationen unterschiedlicher Geheimhaltungsgrade und verschiedener Kategorien von Informationen möglich.

2. Da nicht alle Personen zum Zugriff auf die höchsten Geheimhaltungsgrade berechtigt sind und da nicht alle Personen generell einen berechtigten Informationsbedarf in Bezug auf die im SYSTEM verarbeiteten Informationen haben, muss die sicherheitstechnische Ausgestaltung einen selektiven Zugriff auf Informationen und eine Trennung von Informationen innerhalb des SYSTEMS gewährleisten.

18. INFORMATIONSSICHERHEIT (INFOSEC) bezeichnet die Anwendung von Sicherheitsmaßnahmen zum Schutz von Informationen, die in Kommunikations- und Informationssystemen und anderen elektronischen Systemen verarbeitet, gespeichert oder übermittelt werden, vor dem unabsichtlichen oder absichtlichen Verlust der Vertraulichkeit, Integrität oder Verfügbarkeit, sowie zur Vermeidung des Verlustes der Integrität und Verfügbarkeit der Systeme selbst. INFOSEC-Maßnahmen erstrecken sich auf die Sicherheit von Computern, die Sicherheit der Übertragung, die Sicherheit vor Abstrahlung und die kryptografische Sicherheit sowie die Aufdeckung, Dokumentation und Bekämpfung von Bedrohungen für Informationen und SYSTEME.

19. COMPUTERSICHERHEIT (COMPUSEC) bezeichnet den Einsatz der Sicherheitseigenschaften von Hardware, Firmware und Software eines Computersystems zum Schutz vor unerlaubter Preisgabe, Manipulation, Änderung bzw. Löschung von Informationen sowie vor einem Systemausfall (Denial of Service).

20. COMPUTERSICHERHEITSPRODUKT ist ein allgemeines, der Computersicherheit dienendes Produkt, das zur Integration in ein IT-System und zur Verbesserung bzw. Gewährleistung der Vertraulichkeit, Integrität oder Verfügbarkeit der verarbeiteten Informationen bestimmt ist.

21. KOMMUNIKATIONSSICHERHEIT (COMSEC) bezeichnet die Anwendung von Sicherheitsmaßnahmen auf den Telekommunikationsverkehr, um zu verhindern, dass Unbefugte in den Besitz wertvoller Informationen gelangen, die aus dem Zugriff auf den Telekommunikationsverkehr und dessen Auswertung gewonnen werden könnten, oder um die Authenthizität des Telekommunikationsverkehrs sicherzustellen.

Anmerkung:

Diese Maßnahmen umfassen die kryptografische Sicherheit, die Sicherheit der Übermittlung und die Sicherheit vor Abstrahlung und ferner die verfahrens-, objekt- und personenbezogene Sicherheit sowie die Dokumenten- und Computersicherheit.

▼B

22. EVALUATION bezeichnet die eingehende technische Prüfung der Sicherheitsaspekte eines SYSTEMS oder eines Produkts für kryptografische Sicherheit oder Computersicherheit durch eine zuständige Stelle.

Anmerkungen:

1. Bei der Evaluation wird geprüft, ob die verlangten Sicherheitsfunktionen tatsächlich vorhanden sind und ob sie negative Nebeneffekte haben, und es wird bewertet, inwieweit diese Funktionen verfälscht werden könnten.
2. Bei der Evaluation wird ferner bestimmt, inwieweit die für ein SYSTEM geltenden Sicherheitsanforderungen erfüllt bzw. die geltend gemachten Sicherheitsleistungen eines Computersicherheitsprodukts erbracht werden, und es wird die Vertrauenswürdigkeitsstufe des SYSTEMS oder des Produkts für kryptografische Sicherheit oder Computersicherheit bestimmt.

23. ZERTIFIZIERUNG bezeichnet eine — durch eine unabhängige Überprüfung der Durchführung und der Ergebnisse einer Evaluation gestützte — förmliche Bescheinigung darüber, inwieweit ein SYSTEM die Sicherheitsanforderungen erfüllt oder inwieweit ein Computersicherheitsprodukt vorgegebene Sicherheitsleistungen erbringt.

24. AKKREDITIERUNG bezeichnet die Abnahme und Zulassung eines SYSTEMS zur Verarbeitung von EU-Verschlusssachen in seinem betrieblichen Umfeld.

Anmerkung:

Die Akkreditierung sollte erfolgen, nachdem alle einschlägigen sicherheitsrelevanten Verfahren durchgeführt worden sind und der Schutz der Systemressourcen in ausreichendem Maße sichergestellt worden ist. Die Akkreditierung sollte in der Regel auf der Grundlage der SSRS erfolgen und Folgendes umfassen:

a) Festlegung der Zielvorgaben der Akkreditierung dieses System, insbesondere welche Geheimhaltungsgrade verarbeitet werden sollen und welcher Sicherheitsmodus für das System oder Netz vorgeschlagen wird;

b) Bestandsaufnahme des Risikomanagements, in der Bedrohungen und Schwachstellen benannt und entsprechende Gegenmaßnahmen dargelegt werden;

c) sicherheitsbezogene Betriebsverfahren (SecOP) mit einer detaillierten Beschreibung der vorgesehenen Abläufe (z. B. Betriebsarten und Funktionen) und mit einer Beschreibung der Sicherheitseigenschaften des SYSTEMS, die die Grundlage für die Akkreditierung bildet;

d) Plan für die Implementierung und Aufrechterhaltung der Sicherheitseigenschaften;

e) Plan für die erstmalige und nachfolgende Prüfung, Evaluation und Zertifizierung der System- oder Netzsicherheit;

f) gegebenenfalls Zertifizierung zusammen mit anderen Teilaspekten der Akkreditierung.

25. IT-SYSTEM bezeichnet eine Gesamtheit von Betriebsmitteln, Methoden und Verfahren sowie gegebenenfalls Personal, die zusammenwirken, um Aufgaben der Informationsverarbeitung zu erfüllen.

Anmerkungen:

1. Darunter wird eine Gesamtheit von Einrichtungen verstanden, die zur Verarbeitung von Informationen innerhalb des Systems konfiguriert sind.
2. Diese Systeme können der Abfrage, der Steuerung, der Kontrolle, der Kommunikation und wissenschaftlichen oder administrativen Anwendungen einschließlich der Textverarbeitung dienen.
3. Die Grenzen eines Systems werden im Allgemeinen in Bezug auf die Bestandteile definiert, die der Kontrolle einer einzigen für den Betrieb eines IT-Systems zuständigen Stelle (IT System Operational Authority, ITSOA) unterliegen.
4. Ein IT-System kann Teilsysteme enthalten, von denen einige selbst wiederum IT-Systeme sind.

26. Die SICHERHEITSEIGENSCHAFTEN EINES IT-SYSTEMS umfassen alle Funktionen, Merkmale und Eigenschaften der Hardware, Firmware und Software; dazu gehören die Betriebsverfahren, die Nachvollziehbarkeit, die Zugangs- und Zugriffskontrollen, die IT-Umgebung, die Umgebung dezentraler Terminals bzw. Datenstationen, der vorgegebene Managementrahmen, die physischen Strukturen und Geräte sowie Personal- und Kommunikationskontrollen, die erforderlich sind, um einen annehmbaren Schutz der

▼B

Verschlusssachen sicherzustellen, die in einem IT-System verarbeitet werden sollen.

27. IT-NETZ bezeichnet eine Gesamtheit von geografisch verteilten IT-Systemen, die für den Datenaustausch miteinander verbunden sind; darin eingeschlossen sind die Bestandteile der vernetzten IT-Systeme sowie deren Schnittstelle mit den zugrunde liegenden Daten- oder Kommunikationsnetzen.

Anmerkungen:

1. Ein IT-Netz kann die Funktionen eines oder mehrerer Kommunikationsnetze zum Datenaustausch nutzen; mehrere IT-Netze können die Funktionen eines gemeinsamen Kommunikationsnetzes nutzen.
2. Ein IT-Netz wird als „lokal" bezeichnet, wenn es mehrere am selben Standort befindliche Computer miteinander verbindet.

28. Die SICHERHEITSEIGENSCHAFTEN EINES IT-NETZES umfassen die Sicherheitseigenschaften der einzelnen IT-Systeme, aus denen das Netz besteht, sowie jene zusätzlichen Bestandteile und Eigenschaften, die mit dem Netz als solchem verbunden sind (z. B. Kommunikation im Netz, Mechanismen und Verfahren zur Sicherheitsidentifikation und zur Kennzeichnung, Zugriffskontrollen, Programme und automatische Ereignisprotokolle), und die erforderlich sind, um einen angemessenen Schutz der Verschlusssachen sicherzustellen.

29. IT-UMGEBUNG bezeichnet einen Bereich, in dem sich ein oder mehrere Computer, deren lokale Peripheriegeräte und Speichereinheiten, Steuereinheiten sowie ihnen fest zugeordnete Netz- und Kommunikationseinrichtungen befinden.

Anmerkung:

Nicht eingeschlossen sind davon abgetrennte Bereiche, in denen sich dezentrale Peripheriegeräte oder Terminals bzw. Datenstationen befinden, auch wenn diese an Geräte innerhalb der IT-Umgebung angeschlossen sind.

30. UMGEBUNG VON DEZENTRALEN TERMINALS bzw. DATENSTATIONEN bezeichnet einen Bereich außerhalb einer IT-Umgebung, in dem sich Computer, deren lokale Peripheriegeräte oder Terminals bzw. Datenstationen und alle zugehörigen Kommunikationseinrichtungen befinden.

31. TEMPEST-Schutzmaßnahmen (Transient Electromagnetic Pulse Emanation Standard) bezeichnen Sicherheitsmaßnahmen zum Schutz von Geräten und Kommunikationsinfrastruktur gegen die Preisgabe von Verschlusssachen durch unabsichtliche elektromagnetische Abstrahlung.

Kapitel III

Zuständigkeiten im Sicherheitsbereich

ALLGEMEINES

32. Der Sicherheitsausschuss gemäß Abschnitt 1 Nummer 4 ist auch für INFOSEC-Fragen zuständig. Der Sicherheitsausschuss organisiert seine Tätigkeit so, dass er zu den vorstehenden Punkten sachverständigen Rat geben kann.

33. Im Falle von Sicherheitsproblemen (Zwischenfälle, Verstoß gegen Vorschriften usw.) wird die zuständige einzelstaatliche Behörde und/oder das Sicherheitsbüro des Generalsekretariats des Rates sofort tätig. Alle Probleme werden dem Sicherheitsbüro des Generalsekretariats des Rates gemeldet.

34. Der Generalsekretär/Hohe Vertreter oder gegebenenfalls der Leiter einer dezentralen EU-Einrichtung richten ein INFOSEC-Büro ein, das für die Sicherheitsbehörde Leitlinien für die Implementierung und Kontrolle spezieller Sicherheitseigenschaften als Bestandteile von SYSTEMEN vorgibt.

AKKREDITIERUNGSSTELLE FÜR IT-SICHERHEIT (SAA)

35. Die SAA ist entweder

— eine einzelstaatliche Sicherheitsbehörde (NSA),

— die vom Generalsekretär/Hohen Vertreter bestimmte Stelle,

— die Sicherheitsstelle einer dezentralen EU-Einrichtung oder

— deren abgeordnete bzw. benannte Vertreter, je nachdem, welches SYSTEM akkreditiert werden soll.

▼B

36. Die SAA hat sicherzustellen, dass die SYSTEME dem Sicherheitskonzept des Rates entsprechen. Sie hat unter anderem die Aufgabe, die Verarbeitung von EU-Verschlusssachen bis zu einem bestimmten Geheimhaltungsgrad mit dem betreffenden SYSTEM in seinem betrieblichen Umfeld zu genehmigen. Für das Generalsekretariat des Rates und gegebenenfalls die dezentralen EU-Einrichtungen trägt die SAA die Verantwortung für die Sicherheit im Namen des Generalsekretärs/Hohen Vertreters bzw. im Namen der Leiter der dezentralen Einrichtung.

    Die Zuständigkeit der SAA des Generalsekretariats des Rates erstreckt sich auf alle SYSTEME, die innerhalb der Räumlichkeiten des Generalsekretariats des Rates betrieben werden. SYSTEME und Bestandteile von SYSTEMEN, die in einem Mitgliedstaat betrieben werden, verbleiben in der Zuständigkeit dieses Mitgliedstaats. Wenn unterschiedliche Bestandteile eines SYSTEMS in die Zuständigkeit der SAA des Generalsekretariats des Rates und anderer SAA fallen, ernennen alle Parteien ein gemeinsames Akkreditierungsgremium, dessen Koordinierung die SAA des Generalsekretariats des Rates übernimmt.

INFOSEC-STELLE (IA)

37. Die INFOSEC-Stelle ist für die Tätigkeiten des INFOSEC-Büros verantwortlich. Im Falle des Generalsekretariats des Rates und gegebenenfalls der dezentralen EU-Einrichtungen ist die INFOSEC-Stelle für Folgendes verantwortlich:

    — technische Beratung und Unterstützung der SAA,

    — Unterstützung bei der Entwicklung der SSRS,

    — Überprüfung der SSRS im Hinblick auf deren Konsistenz mit diesen Sicherheitsvorschriften und den Dokumenten betreffend die INFOSEC-Politik und -Architektur,

    — gegebenenfalls Teilnahme an den Sitzungen der Akkreditierungsgremien bzw. -ausschüsse und Erstellung von INFOSEC-Empfehlungen für die SAA betreffend Akkreditierung,

    — Unterstützung bei Schulungs- und Ausbildungsmaßnahmen im INFOSEC-Bereich,

    — technische Beratung bei der Untersuchung von Zwischenfällen im INFOSEC-Bereich,

    — Erstellung technischer strategischer Leitlinien, um sicherzustellen, dass nur zugelassene Software verwendet wird.

FÜR DEN BETRIEB EINES IT-SYSTEMS ZUSTÄNDIGE STELLE (ITSOA)

38. Die INFOSEC-Stelle delegiert zum frühestmöglichen Zeitpunkt die Verantwortung für die Implementierung und die Anwendung von Kontrollen und speziellen Sicherheitseigenschaften des SYSTEMS an die für den Betrieb des IT-SYSTEMS zuständige Stelle (IT System Operational Authority, ITSOA). Diese Verantwortung besteht während der gesamten Lebensdauer des SYSTEMS von der Konzeption des Projekts bis zur endgültigen Entsorgung.

39. Die ITSOA ist verantwortlich für alle Sicherheitsmaßnahmen, die als Teil des gesamten SYSTEMS konzipiert sind. Diese Verantwortung schließt die Erstellung von sicherheitsrelevanten Betriebsverfahren (Security Operating Procedures, SecOPs) ein. Die ITSOA legt die Sicherheitsstandards- und verfahren fest, die vom Lieferanten des SYSTEMS eingehalten werden müssen.

40. Die ITSOA kann gegebenenfalls einen Teil ihrer Verantwortung delegieren, z. B. an den INFOSEC-Sicherheitsbeamten bzw. den für den Standort zuständigen INFOSEC-Sicherheitsbeamten. Die verschiedenen INFOSEC-Aufgaben können von einer einzigen Person wahrgenommen werden.

NUTZER

41. Alle Nutzer müssen sicherstellen, dass ihr Handeln die Sicherheit des von ihnen verwendeten SYSTEMS nicht beeinträchtigt.

INFOSEC-SCHULUNG

42. Ausbildung und Schulung im INFOSEC-Bereich wird je nach Sachlage auf den verschiedenen Ebenen und für unterschiedliches Personal innerhalb des Generalsekretariats des Rates, der dezentralen EU-Einrichtungen oder der Behörden der Mitgliedstaaten angeboten.

▼B

Kapitel IV

Nichttechnische Sicherheitsmaßnahmen

PERSONALBEZOGENE SICHERHEIT

43. Nutzer des SYSTEMS müssen sich erfolgreich einer Sicherheitsüberprüfung unterzogen haben, die dem Geheimhaltungsgrad der in ihrem bestimmten SYSTEM verarbeiteten Informationen entspricht, und sie müssen einen entsprechenden berechtigten Informationsbedarf haben. Der Zugang zu bestimmten Einrichtungen oder Informationen, die für die SYSTEME sicherheitsrelevant sind, erfordert eine besondere Ermächtigung, die gemäß den Verfahren des Rates erteilt wird.

44. Die SAA benennt alle sicherheitskritischen Arbeitsplätze und legt fest, welcher Sicherheitsüberprüfung und Überwachung sich alle Personen an diesen Arbeitsplätzen unterziehen müssen.

45. SYSTEME werden so spezifiziert und konzipiert, dass die Zuweisung von Aufgaben und Zuständigkeiten erleichtert wird und dass vermieden wird, dass eine einzige Person umfassende Kenntnis oder Kontrolle über die für die Systemsicherheit entscheidenden Punkte erhält. Damit wird bezweckt, dass für eine Änderung oder absichtliche Schädigung des Systems oder Netzes eine Absprache zwischen zwei oder mehr Personen erforderlich wäre.

MATERIELLE SICHERHEIT

46. IT-Umgebungen und Umgebungen von dezentralen Terminals bzw. Datenstationen (gemäß den Nummern 29 und 30), in denen als „CONFIDENTIEL UE“ und höher eingestufte Informationen mit informationstechnischen Mitteln verarbeitet werden oder in denen der Zugriff auf solche Informationen potenziell möglich ist, werden je nach Sachlage als EU-Sicherheitsbereiche der Kategorie I oder II bzw. gemäß deren einzelstaatlichen Entsprechungen eingestuft.

47. IT-Umgebungen und Umgebungen von dezentralen Terminals bzw. Datenstationen, in denen die Sicherheit des SYSTEMS beeinflusst werden kann, dürfen nicht mit nur einem befugten Beamten oder sonstigen Bediensteten besetzt werden.

KONTROLLE DES ZUGANGS ZU EINEM SYSTEM

48. Alle Informationen und jegliches Material, das die Kontrolle des Zugangs zu einem SYSTEM ermöglicht, werden durch Vorkehrungen geschützt, die dem höchsten Geheimhaltungsgrad und der Kategorie von Informationen, zu denen sie Zugang gewähren könnten, entsprechen.

49. Informationen und Material zur Zugangskontrolle werden gemäß den Nummern 61 bis 63 vernichtet, wenn sie nicht mehr zu diesem Zweck verwendet werden.

Kapitel V

Technische Sicherheitsmaßnahmen

INFORMATIONSSICHERHEIT

50. Der Urheber einer Information hat die Aufgabe, alle informationstragenden Dokumente zu identifizieren und ihnen einen Geheimhaltungsgrad zuzuordnen, unabhängig davon, ob sie als Papierausdruck oder auf einem elektronischen Datenträger vorliegen. Auf jeder Seite eines Papierausdrucks wird oben und unten der Geheimhaltungsgrad vermerkt. Jeder Ausgabe, ob als Papierausdruck oder auf einem elektronischen Datenträger, wird der höchste Geheimhaltungsgrad der zu ihrer Erstellung verarbeiteten Informationen zugeordnet. Die Betriebsart eines SYSTEMS kann den Geheimhaltungsgrad für Ausgaben dieses Systems ebenfalls beeinflussen.

51. Eine Organisation und ihre Informationsträger müssen sich mit der Problematik der Zusammenstellung einzelner Informationsbestandteile und den Schlussfolgerungen, die aus den miteinander verknüpften Bestandteilen gewonnen werden können, auseinander setzen und entscheiden, ob die Gesamtheit der Informationen höher eingestuft werden muss oder nicht.

52. Die Tatsache, dass die Information in einer Kurzform, als Übertragungscode oder in einer beliebigen binären Darstellung vorliegt, bietet keinen Schutz und sollte deshalb die Einstufung der Information nicht beeinflussen.

53. Wenn Informationen von einem SYSTEM zu einem anderen übertragen werden, werden diese Informationen bei der Übertragung und im

▼B

Empfängersystem entsprechend dem ursprünglichen Geheimhaltungsgrad und der ursprünglichen Kategorie geschützt.

54. Die Behandlung aller elektronischen Datenträger muss dem höchsten Geheimhaltungsgrad der gespeicherten Informationen bzw. der Datenträger-Kennzeichnung entsprechen; elektronische Datenträger müssen jederzeit angemessen geschützt werden.

55. Wieder verwendbare elektronische Datenträger, die zur Speicherung von EU-Verschlusssachen verwendet werden, behalten den höchsten Geheimhaltungsgrad bei, für den sie jemals verwendet wurden, bis diese Informationen ordnungsgemäß herabgestuft worden sind oder der Geheimhaltungsgrad aufgehoben wurde und der Datenträger entsprechend neu eingestuft beziehungsweise der Geheimhaltungsgrad aufgehoben oder durch ein zugelassenes Verfahren des Generalsekretariats des Rates oder eines Mitgliedstaats vernichtet wurde (siehe Nummern 61 bis 63).

KONTROLLE UND NACHVOLLZIEHBARKEIT IN BEZUG AUF INFORMATIONEN

56. Der Zugriff auf Informationen, die als „SECRET UE“ und höher eingestuft sind, wird automatisch („audit trails“) oder manuell protokolliert und dokumentiert. Die Protokolle werden im Einklang mit diesen Sicherheitsvorschriften aufbewahrt.

57. EU-Verschlusssachen, die als Ausgaben innerhalb der IT-Umgebung vorliegen, können als eine einzige Verschlusssache behandelt werden und brauchen nicht registriert zu werden, sofern sie in geeigneter Weise identifiziert, mit dem Geheimhaltungsgrad gekennzeichnet und angemessen kontrolliert werden.

58. Für die Fälle, in denen ein SYSTEM, in dem EU-Verschlusssachen verarbeitet werden, Ausgaben erstellt und diese Ausgaben aus einer IT-Umgebung in die Umgebung von dezentralen Terminals bzw. Datenstationen übermittelt werden, werden — von der SAA genehmigte — Verfahren festgelegt, um die Ausgabe an den dezentralen Standorten zu kontrollieren. Für Informationen, die als „SECRET UE“ oder höher eingestuft sind, beinhalten diese Verfahren besondere Anweisungen für die Nachvollziehbarkeit in Bezug auf diese Informationen.

BEHANDLUNG UND KONTROLLE VON AUSTAUSCHBAREN ELEKTRONISCHEN DATENTRÄGERN

59. Alle austauschbaren elektronischen Datenträger, die als „CONFIDENTIEL UE“ und höher eingestuft sind, werden als Material angesehen und unterliegen den allgemeinen Regeln. Die Identifizierung und Kennzeichnung des Geheimhaltungsgrades muss an das besondere physische Erscheinungsbild der Datenträger angepasst werden, so dass diese eindeutig erkannt werden können.

60. Die Nutzer sind dafür verantwortlich, dass EU-Verschlusssachen auf Datenträgern gespeichert werden, die korrekt mit dem Geheimhaltungsgrad gekennzeichnet sind und angemessen geschützt werden. Um sicherzustellen, dass die Speicherung von Informationen auf elektronischen Datenträgern für alle EU-Geheimhaltungsgrade im Einklang mit diesen Sicherheitsvorschriften erfolgt, werden entsprechende Verfahren festgelegt.

FREIGABE UND VERNICHTUNG VON ELEKTRONISCHEN DATENTRÄGERN

61. Elektronische Datenträger, die zur Speicherung von EU-Verschlusssachen verwendet werden, können herabgestuft werden oder ihr Geheimhaltungsgrad kann aufgehoben werden, sofern Verfahren angewandt werden, die vom Generalsekretariat des Rates oder einem Mitgliedstaat zugelassen sind.

62. Elektronische Datenträger, die Informationen des Geheimhaltungsgrades „TRÈS SECRET UE/EU TOP SECRET“ oder Informationen spezieller Kategorien enthalten haben, werden nicht freigegeben oder wiederverwendet.

63. Wenn elektronische Datenträger nicht freigegeben werden können oder nicht wiederverwendbar sind, werden sie nach einem vom Generalsekretariat des Rates oder einem Mitgliedstaat zugelassenen Verfahren vernichtet.

KOMMUNIKATIONSSICHERHEIT

64. Wenn EU-Verschlusssachen elektromagnetisch übermittelt werden, werden besondere Maßnahmen zum Schutz von Vertraulichkeit, Integrität und Verfügbarkeit solcher Übermittlungsvorgänge ergriffen. Die SAA legt die Anforderungen an den Schutz von Übermittlungsvorgängen vor Aufdek-

▼B

kungs- und Abhörmaßnahmen fest. Der Schutz von Informationen, die in einem Kommunikationssystem übermittelt werden, richtet sich nach den Anforderungen an die Vertraulichkeit, Integrität und Verfügbarkeit.

65. Wenn zum Schutz von Vertraulichkeit, Integrität und Verfügbarkeit kryptografische Methoden erforderlich sind, werden diese Methoden oder damit verbundene Produkte speziell zu diesem Zweck von der SAA zugelassen.

66. Während der Übermittlung wird die Vertraulichkeit von als „SECRET UE“ und höher eingestuften Informationen durch kryptografische Methoden oder Produkte geschützt, die vom Rat auf Empfehlung des Sicherheitsausschusses des Rates zugelassen worden sind. Während der Übermittlung wird die Vertraulichkeit von Informationen des Geheimhaltungsgrades „CONFIDENTIEL UE“ oder „RESTREINT UE“ durch kryptografische Methoden oder Produkte geschützt, die entweder vom Generalsekretär/Hohen Vertreter auf Empfehlung des Sicherheitsausschusses des Rates oder von einem Mitgliedstaat zugelassen worden sind.

67. Detaillierte Regeln für die Übermittlung von EU-Verschlusssachen werden in besonderen Sicherheitsanweisungen festgelegt, die vom Rat auf Empfehlung des Sicherheitsausschusses des Rates erlassen werden.

68. Unter außergewöhnlichen Betriebsbedingungen können Informationen der Geheimhaltungsgrade „RESTREINT UE“, „CONFIDENTIEL UE“ und „SECRET UE“ als Klartext übermittelt werden, sofern dies in jedem einzelnen Fall ausdrücklich genehmigt wird. Solche außergewöhnlichen Bedingungen sind gegeben

    a) während einer drohenden oder aktuellen Krisen-, Konflikt- oder Kriegssituation und

    b) wenn die Schnelligkeit der Zustellung von vordringlicher Bedeutung ist und keine Verschlüsselungsmittel verfügbar sind und wenn davon ausgegangen wird, dass die übermittelte Information nicht rechtzeitig dazu missbraucht werden kann, Vorgänge negativ zu beeinflussen.

69. Ein SYSTEM muss in der Lage sein, bei Bedarf den Zugriff auf EU-Verschlusssachen an einzelnen oder allen seiner dezentralen Datenstationen bzw. Terminals zu verweigern, und zwar entweder durch eine physische Abschaltung oder durch spezielle, von der SAA genehmigte Softwarefunktionen.

SICHERHEIT DER INSTALLATION UND SICHERHEIT VOR ABSTRAHLUNG

70. Die Erstinstallation von SYSTEMEN und nachfolgende größere Änderungen werden so geregelt, dass die Arbeiten von sicherheitsüberprüften Personen durchgeführt und ständig durch technisch qualifiziertes Personal überwacht werden, das zum Zugang zu EU-Verschlusssachen des höchsten im SYSTEM voraussichtlich gespeicherten und verarbeiteten Geheimhaltungsgrades ermächtigt ist.

71. Alle Einrichtungen werden im Einklang mit dem aktuellen Sicherheitskonzept des Rates installiert.

72. SYSTEME, in denen als „CONFIDENTIEL UE“ und höher eingestufte Informationen verarbeitet werden, werden so geschützt, dass ihre Sicherheit nicht durch kompromittierende Abstrahlung bedroht werden kann, wobei entsprechende Analyse- und Kontrollmaßnahmen als „TEMPEST“ bezeichnet werden.

73. TEMPEST-Gegenmaßnahmen bei Installationen im Generalsekretariat des Rates und in dezentralen EU-Einrichtungen werden von einer für TEMPEST zuständigen Stelle überprüft und genehmigt, die von der Sicherheitsstelle des Generalsekretariats des Rates bestimmt wird. Im Falle einzelstaatlicher Einrichtungen, in denen EU-Verschlusssachen verarbeitet werden, ist die anerkannte nationale TEMPEST-Zulassungsstelle für die Genehmigung zuständig.

Kapitel VI

Sicherheit bei der Verarbeitung

SICHERHEITSBEZOGENE BETRIEBSVERFAHREN

74. In den sicherheitsbezogenen Betriebsverfahren (SecOPs) werden die in Sicherheitsfragen geltenden Grundsätze, die einzuhaltenden Betriebsverfahren sowie die Zuständigkeiten des Personals festgelegt. Für die Erstellung der sicherheitsbezogenen Betriebsverfahren ist die für den Betrieb des IT-Systems zuständige Stelle (ITSOA) verantwortlich.

▼B

SOFTWARESCHUTZ UND KONFIGURATIONSMANAGEMENT

75. Der Schutz von Anwendungsprogrammen wird auf der Grundlage einer Bewertung der Sicherheitseinstufung des Programms selbst festgelegt, und nicht aufgrund der Einstufung der zu verarbeitenden Informationen. Die benutzten Software-Versionen sollten in regelmäßigen Abständen überprüft werden, um ihre Integrität und korrekte Funktion sicherzustellen.

76. Neue oder geänderte Versionen einer Software sollten erst für die Verarbeitung von EU-Verschlusssachen benutzt werden, wenn sie von der ITSOA geprüft worden sind.

PRÜFUNG AUF DAS VORHANDENSEIN VON PROGRAMMEN MIT SCHADENSFUNKTIONEN UND VON COMPUTERVIREN

77. Die Prüfung auf das Vorhandensein von Programmen mit Schadensfunktionen und von Computerviren wird regelmäßig durchgeführt, und zwar im Einklang mit den Anforderungen der SAA.

78. Alle elektronischen Datenträger, die im Generalsekretariat des Rates, in dezentralen EU-Einrichtungen oder in Stellen der Mitgliedstaaten eingehen, sollten auf das Vorhandensein von Programmen mit Schadensfunktionen und von Computerviren überprüft werden, bevor sie in ein SYSTEM eingebracht werden.

WARTUNG

79. In Verträgen und Verfahrensanweisungen für die planmäßige und außerplanmäßige Wartung von SYSTEMEN, für die eine SSRS erstellt worden ist, werden Anforderungen und Vorkehrungen für den Zutritt von Wartungspersonal zu einer IT-Umgebung und für die zugehörige Wartungsausrüstung festgelegt.

80. Die Anforderungen werden in der SSRS und die Verfahren in den SecOPs präzise festgelegt. Wartungsarbeiten durch einen Auftragnehmer, die Diagnoseverfahren mit Fernzugriff erfordern, sind nur unter außergewöhnlichen Umständen und unter strenger Sicherheitskontrolle und nur nach Genehmigung durch die SAA zulässig.

Kapitel VII

Beschaffungswesen

81. Jedes zu beschaffende Sicherheitsprodukt, das zusammen mit dem SYSTEM verwendet werden soll, sollte auf der Grundlage international anerkannter Kriterien (wie z. B. Common Criteria for Information Technology Security Evaluation, ISO 15408) entweder bereits evaluiert und zertifiziert sein oder sich in der Phase der Evaluation und Zertifizierung durch eine geeignete Evaluations- und Zertifizierungsstelle befinden.

82. Bei der Überlegung, ob Ausrüstung, insbesondere elektronische Speichermedien, eher geleast als gekauft werden soll, sollte berücksichtigt werden, dass diese Ausrüstung, sobald sie zur Verarbeitung von EU-Verschlusssachen verwendet wurde, nicht mehr aus einem angemessen sicheren Umfeld herausgegeben werden kann, ohne dass sie zuvor mit Zustimmung der SAA freigegeben worden ist, und dass diese Zustimmung eventuell nicht immer gegeben werden kann.

AKKREDITIERUNG

83. Alle SYSTEME, für die eine SSRS erstellt werden muss, müssen von der SAA akkreditiert werden, bevor EU-Verschlusssachen damit verarbeitet werden, und zwar auf der Grundlage der Angaben in der SSRS, in den SecOPs und in anderer relevanter Dokumentation. Teilsysteme und dezentrale Terminals bzw. Datenstationen werden als Teil aller SYSTEME akkreditiert, mit denen sie verbunden sind. Wenn ein SYSTEM sowohl vom Rat als auch von anderen Organisationen genutzt wird, nehmen das Generalsekretariat des Rates und die relevanten Sicherheitsstellen die Akkreditierung einvernehmlich vor.

84. Die Akkreditierung kann gemäß einer für das jeweilige SYSTEM geeigneten und von der SAA definierten Akkreditierungsstrategie durchgeführt werden.

EVALUATION UND ZERTIFIZIERUNG

85. Vor der Akkreditierung werden in bestimmten Fällen die Sicherheitseigenschaften der Hardware, Firmware und Software eines SYSTEMS evaluiert und daraufhin zertifiziert, dass sie in der Lage sind, Informationen des beabsichtigten Geheimhaltungsgrades zu schützen.

▼B

86. Die Anforderungen für Evaluation und Zertifizierung werden in die Systemplanung einbezogen und in der SSRS präzise festgelegt.

87. Die Evaluation und Zertifizierung wird gemäß genehmigter Leitlinien und von technisch qualifiziertem und ausreichend sicherheitsüberprüftem Personal durchgeführt, das im Auftrag der ITSOA tätig wird.

88. Das betreffende Personal kann von einer benannten Evaluations- und Zertifizierungsstelle eines Mitgliedstaates oder dessen benannten Vertretern, z. B. einem fachkundigen und ermächtigten Vertragspartner, bereitgestellt werden.

89. Wenn die SYSTEME auf bestehenden, einzelstaatlich evaluierten und zertifizierten Computersicherheitsprodukten beruhen, kann die Evaluation und die Zertifizierung vereinfacht werden (z. B. durch Beschränkung auf Integrationsaspekte).

REGELMÄSSIGE ÜBERPRÜFUNG VON SICHERHEITSEIGENSCHAFTEN ZUR AUFRECHTERHALTUNG DER AKKREDITIERUNG

90. Die ITSOA legt Verfahren für eine regelmäßige Kontrolle fest, durch die garantiert wird, dass alle Sicherheitseigenschaften des SYSTEMS noch ordnungsgemäß vorhanden sind.

91. Welche Änderungen eine neue Akkreditierung bzw. die vorherige Genehmigung durch die SAA erfordern, wird in der SSRS präzise festgelegt. Nach jeder Änderung, Instandsetzung oder Störung, die sich auf die Sicherheitseigenschaften des SYSTEMS ausgewirkt haben könnte, sorgt die ITSOA dafür, dass eine Überprüfung durchgeführt wird, um die korrekte Funktion der Sicherheitseigenschaften sicherzustellen. Eine Aufrechterhaltung der Akkreditierung des Systems hängt normalerweise vom zufrieden stellenden Ergebnis dieser Überprüfung ab.

92. Alle SYSTEME, die Sicherheitseigenschaften aufweisen, werden regelmäßig von der SAA kontrolliert oder überprüft. Bei SYSTEMEN, die Informationen des Geheimhaltungsgrades „TRÈS SECRET UE/EU TOP SECRET“ oder Informationen mit zusätzlichen Kennzeichnungen verarbeiten, werden die Kontrollen mindestens einmal jährlich durchgeführt.

Kapitel VIII

Zeitlich befristete oder gelegentliche Nutzung

SICHERHEIT VON MIKROCOMPUTERN BZW. PCs

93. Mikrocomputer bzw. PCs mit eingebauten Speicherplatten (oder anderen nichtflüchtigen Datenträgern), die als Einzelrechner oder in einem Netz betrieben werden, sowie tragbare Computer (z. B. tragbare PCs und Notebook-Computer) mit eingebauten Festplatten werden im selben Sinne wie Disketten oder andere austauschbare elektronische Datenträger als Speichermedium für Informationen eingestuft.

94. Der Schutz dieser Geräte muss in Bezug auf Zugang, Verarbeitung, Speicherung und Transport dem höchsten Geheimhaltungsgrad der jemals gespeicherten oder verarbeiteten Informationen entsprechen (bis zur Herabstufung oder Aufhebung des Geheimhaltungsgrades gemäß genehmigter Verfahren).

NUTZUNG VON PRIVATER IT-AUSRÜSTUNG FÜR DIENSTLICHE ZWECKE DES RATES

95. Die Nutzung von privaten austauschbaren elektronischen Datenträgern, privater Software und IT-Hardware mit Speichermöglichkeit (z. B. PCs und tragbare Computer) zur Verarbeitung von EU-Verschlusssachen ist untersagt.

96. Private Hardware, Software und Speichermedien dürfen in Bereiche der Kategorien I oder II, in denen EU-Verschlusssachen verarbeitet werden, nur mit Erlaubnis des Leiters des Sicherheitsbüros des Generalsekretariats des Rates, einer Stelle eines Mitgliedstaats oder der jeweiligen dezentralen EU-Einrichtung verbracht werden.

NUTZUNG VON IT-AUSRÜSTUNG EINES AUFTRAGNEHMERS ODER EINES MITGLIEDSTAATS FÜR DIENSTLICHE ZWECKE DES RATES

97. Die Nutzung von IT-Ausrüstung und Software eines Auftragnehmers für dienstliche Zwecke des Rates kann vom Leiter des Sicherheitsbüros des Generalsekretariats des Rates, einer einzelstaatlichen Stelle oder der jeweiligen dezentralen EU-Einrichtung genehmigt werden. Die Verwendung der IT-Ausrüstung und Software eines Mitgliedstaats durch Bedienstete des

▼B

Generalsekretariats des Rates oder einer dezentralen EU-Einrichtung kann ebenfalls erlaubt werden; in diesem Fall unterliegt die IT-Ausrüstung der jeweiligen Bestandskontrolle des Generalsekretariats des Rates. Wenn die IT-Ausrüstung zur Verarbeitung von EU-Verschlusssachen verwendet werden soll, wird in jedem Fall die zuständige SAA konsultiert, damit die INFOSEC-Aspekte, die auf die Nutzung dieser Ausrüstung anwendbar sind, angemessen berücksichtigt und umgesetzt werden.

▼B

ABSCHNITT XII

WEITERGABE VON EU-VERSCHLUSSSACHEN AN DRITTSTAATEN ODER INTERNATIONALE ORGANISATIONEN

GRUNDSÄTZE FÜR DIE WEITERGABE VON EU-VERSCHLUSSSACHEN

1. Über die Weitergabe von EU-Verschlusssachen an Drittstaaten oder internationale Organisationen beschließt der Rat nach Maßgabe

   — von Art und Inhalt dieser Verschlusssachen;

   — des Grundsatzes „Kenntnis nur wenn nötig“;

   — der Vorteile für die EU.

   Der Mitgliedstaat, aus dem die EU-Verschlusssache stammt, die weitergegeben werden soll, wird um Zustimmung ersucht.

2. Einschlägige Beschlüsse werden von Fall zu Fall gefasst und richten sich nach

   — dem gewünschten Maß an Zusammenarbeit mit den betreffenden Drittstaaten oder internationalen Organisationen;

   — deren Vertrauenswürdigkeit, die nach dem Geheimhaltungsgrad, der für die diesen Staaten oder Organisationen anvertrauten Verschlusssachen vorgesehen würde, und nach der Vereinbarkeit der dort geltenden Sicherheitsvorschriften mit den Sicherheitsvorschriften der EU zu bemessen ist; der Sicherheitsausschuss des Rates gibt dazu für den Rat ein technisches Gutachten ab.

3. Durch die Annahme von EU-Verschlusssachen verpflichten sich die betreffenden Drittstaaten oder internationalen Organisationen, die übermittelten Informationen nur zu den Zwecken zu verwenden, für die die Weitergabe oder der Austausch von Informationen beantragt worden ist, und den vom Rat verlangten Schutz zu bieten.

KOOPERATIONSSTUFEN

4. Hat der Rat beschlossen, die Weitergabe oder den Austausch von Verschlusssachen im Falle eines bestimmten Staates oder einer internationalen Organisation zu gestatten, so legt er außerdem fest, wie weit diese Zusammenarbeit gehen kann. Dies hängt insbesondere von dem Sicherheitskonzept und den Sicherheitsvorschriften dieses Staates oder dieser Organisation ab.

5. Es gibt drei Kooperationsstufen:

   Stufe 1

   Zusammenarbeit mit Drittstaaten oder internationalen Organisationen, deren Sicherheitskonzept und -vorschriften sehr weitgehend mit denen der EU übereinstimmen;

   Stufe 2

   Zusammenarbeit mit Drittstaaten oder internationalen Organisationen, deren Sicherheitskonzept und -vorschriften deutlich von denen der EU abweichen;

   Stufe 3

   Gelegentliche Zusammenarbeit mit Drittstaaten oder internationalen Organisationen, deren Sicherheitskonzept und -vorschriften nicht eingeschätzt werden können.

6. Die Sicherheitsvorschriften, die angesichts des technischen Gutachtens des Sicherheitsausschusses des Rates im Einzelfall angepasst werden und deren Anwendung von den Empfängern zum Schutz der an sie weitergegebenen Verschlusssachen verlangt wird, richten sich nach den verschiedenen Kooperationsstufen. Diese Verfahren und Sicherheitsvorschriften sind in den Anhängen 4, 5 und 6 detailliert dargelegt.

ABKOMMEN

7. Beschließt der Rat, dass ein ständiger oder langfristiger Austausch von Verschlusssachen zwischen der EU und Drittstaaten oder anderen internationalen Organisationen erforderlich ist, so arbeitet er mit diesen „Abkommen über die Sicherheitsverfahren für den Austausch von Verschlusssachen“ aus, die das Ziel der Zusammenarbeit und die gegenseitigen Vorschriften für den Schutz der ausgetauschten Informationen festlegen.

8. Für den Fall einer gelegentlichen Zusammenarbeit im Rahmen der Stufe 3, die per Definition zeitlich und sachlich begrenzt ist, kann eine einfache Vereinbarung, die die Art der auszutauschenden Verschlusssache und die gegenseitigen Verpflichtungen festlegt, an die Stelle des „Abkommens über

▼B

die Sicherheitsverfahren für den Austausch von Verschlusssachen“ treten, sofern die Verschlusssache nicht höher als „RESTREINT UE“ eingestuft ist.

9. Die Entwürfe für Abkommen über die Sicherheitsverfahren oder für Vereinbarungen werden vom Sicherheitsausschuss gebilligt, bevor sie dem Rat zur Entscheidung vorgelegt werden.

10. Die nationalen Sicherheitsbehörden gewähren dem Generalsekretär/Hohen Vertreter alle erforderliche Unterstützung, damit sichergestellt ist, dass die Informationen, die weitergegeben werden sollen, gemäß den Bestimmungen der Abkommen über die Sicherheitsverfahren oder der betreffenden Vereinbarungen genutzt und geschützt werden.

▼B

Anhang 1

Verzeichnis der nationalen Sicherheitsbehörden

▼M1

BELGIEN

Service public fédéral des affaires étrangères, du commerce extérieur et de la coopération au développement
Autorité nationale de sécurité (ANS)
Direction du protocole et de la sécurité
Service de la sécurité P & S 6
Rue des Petits Carmes 15
B-1000 Bruxelles

Federale Overheidsdienst Buitenlandse Zaken, Buitenlandse Handel en Ontwikkelingssamenwerking
Nationale Veiligheidsoverheid (NVO)
Directie Protocol en Veiligheid P&S 6
Karmelietenstraat 15
B-1000 Brussel
Téléphone du secrétariat: (32-2) 519 05 74
Téléphone de la présidence: (32-2) 501 82 20; (32-2) 501 87 10
Télécopieur: (32-2) 519 05 96

TSCHECHISCHE REPUBLIK

National Security Authority
Na Popelce 2/16
CZ-150 06 Praha 56
Telefon: (420) 257 28 33 35
Fax: (420) 257 28 31 10

DÄNEMARK

Politiets Efterretningstjeneste
Klausdalsbrovej 1
DK-2860 Søborg
Telefon (45) 33 14 88 88
Fax (45) 33 43 01 90

DEUTSCHLAND

Bundesministerium des Innern
Referat IS 2
Alt-Moabit 101 D
D-11014 Berlin
Telefon: 49-18 88–681-15 26
Fax: 49-18 88-681-558 06

ESTLAND

Ministry of Defence, Republic of Estonia, Department of Security
Sakala 1
EE-15094 Tallinn
Telefon: (372) 717 00 30
Fax: (372) 717 00 01

GRIECHENLAND

Γενικό Επιτελείο Εθνικής Άμυνας (ΓΕΕΘΑ)
Υπηρεσία Στρατιωτικών Πληροφοριών (ΥΣΠ — Β Κλάδος)
Τμήμα Ασφαλείας και Αντιπληροφοριών
ΣΤΓ 1020-Χολαργός (Αθήνα)
Ελλάδα
Τηλέφωνα: (30) 210 657 20 09 (ώρες γραφείου), (30) 210 657 20 10 (ώρες γραφείου)
Φαξ: (30) 210 642 64 32, (30) 210 657 21 81

Hellenic National Defence General Staff (HNDGS)
Military Intelligence Service (MIS-Bi Branch)
Security Counterintelligence Section
GR-STG 1020 Holargos — Athens
Telephone: (30) 210 657 20 09, (30) 210 657 20 10
Fax: (30) 210 642 64 32, (30) 210 657 21 81

▼**M1**

SPANIEN

Autoridad Nacional de Seguridad
Oficina Nacional de Seguridad
Avenida Padre Huidobro s/n
Carretera Nacional Radial VI, km 8,5
E-28023 Madrid
Teléfono: (34-91) 372 57 07, (34-91) 372 50 27
Fax: (34-91) 372 58 08

FRANKREICH

Secrétariat général de la défense nationale
Service de sécurité et de défense (SGDN/SSD)
51 boulevard de la Tour-Maubourg
F-75700 Paris 07 SP
Téléphone: (33-1) 71 75 81 77
Télécopieur: (33-1) 71 75 82 00

IRLAND

National Security Authority
Department of Foreign Affairs
80 St. Stephens Green
Dublin 2
Ireland
Telephone: (353-1) 478 08 22
Fax: (353-1) 478 14 84

ITALIEN

Presidenza del Consiglio dei Ministri
Autorità Nazionale per la Sicurezza
Ufficio Centrale per la Sicurezza
Via della Pineta Sacchetti, 216
I-00168 Roma
Tel.: (39) 066 27 47 75
Fax: (39) 066 14 33 97

ZYPERN

Υπουργείο Άμυνας
Στρατιωτικό επιτελείο του υπουργού
Εθνική Αρχή Ασφάλειας (ΕΑΑ)
Υπουργείο Άμυνας
Λεωφόρος Εμμανουήλ Ροΐδη 4
1432 Λευκωσία, Κύπρος
Τηλέφωνα: (357) 22 80 75 69, (357) 22 80 75 19, (357) 22 80 77 64
Φαξ: (357) 22 30 23 51

Ministry of Defence
Minister's Military Staff
National Security Authority (NSA)
4 Emanuel Roidi street
CY-1432 Nicosia
Telephone: (357) 22 80 75 69; (357) 22 80 75 19; (357) 22 80 77 64
Fax: (357) 22 30 23 51

LETTLAND

Constitution Protection Bureau of the Republic of Latvia
Miera Iela 85/A
LV-1001 Riga
Telefon: (371) 702 54 18
Fax: (371) 702 54 06

LITAUEN

National Security Authority of the Republic of Lithuania
Gedimino 40/2
LT-2600 Vilnius
Telefon: (370-5) 266 32 05
Fax: (370-5) 266 32 00

LUXEMBURG

Autorité nationale de sécurité
Ministère d'État

▼**M1**

Boîte Postale 23 79
L-1023 Luxembourg
Téléphone: (352) 478 22 10 (central), (352) 478 22 35 (ligne directe)
Télécopieur: (352) 478 22 43; (352) 478 22 71

UNGARN

National Security Authority Republic of Hungary
Pf. 2
HU-1352 Budapest
Telefon: (361) 346 96 52
Fax: (361) 346 96 58

MALTA

Ministry of Justice and Home Affairs
P.O. Box 146
MT-Valletta
Telefon: (356) 21 24 98 44
Fax: (356) 21 23 53 00

NIEDERLANDE

Ministerie van Binnenlandse Zaken
Postbus 200102500 EA Den Haag
Nederland
Tel.: (31-70) 320 44 00
Fax: (31-70) 320 07 33

Ministerie van Defensie
Militaire Inlichtingendienst (MID)
Postbus 207012500 ES Den Haag
Nederland
Tel.: (31-70) 318 70 60
Fax: (31-70) 318 79 51

ÖSTERREICH

Informationssicherheitskommission
Bundeskanzleramt
Ballhausplatz 2
A-1014 Wien
Telefon: 431-531 15 23 96
Fax: 431-531 15 25 08

POLEN

Military Information Services
National Security Authority — Military Sphere
PL-00-909 Warszawa 60
Telefon: (48-22) 684 61 19
Fax: (48-22) 684 61 72

Internal Security Agency
Department for the Protection of Classified Information
2A Rakowiecka St.
PL-00-993 Warszawa
Telefon: (48-22) 585 73 60
Fax: (48-22) 585 85 09

PORTUGAL

Presidência do Conselho de Ministros
Autoridade Nacional de Segurança
Avenida Ilha da Madeira
P-1400-204 Lisboa
Tel.: (351-21) 301 17 10
Fax: (351-21) 303 17 11

SLOWENIEN

Office of the Government of the Republic of Slovenia
For the Protection of Classified Information — NSA
Slovenska cesta 5
SVN-1000 Ljubljana
Telefon: (386-1) 426 91 20
Fax: (386-1) 426 91 91

▼**M1**

SLOWAKEI

National Security Authority
Budatínska 30
SK-851 05 Bratislava
Telefon: (421-2) 68 69 95 09
Fax: (421-2) 63 82 40 05

FINNLAND

Ulkoasiainministeriö/Utrikesministeriet
Alivaltiosihteeri (Hallinto)/Understatssekreteraren (Administration)
Laivastokatu/Maringatan 22
PL/PB 176
FI-00161 Helsinki/Helsingfors
P. (358-9) 16 05 53 38
F. (358-9) 16 05 53 03

SCHWEDEN

Utrikesdepartementet
SSSB
S-103 39 Stockholm
Telefon (46-8) 405 54 44
Fax (46-8) 723 11 76

VEREINIGTES KÖNIGREICH

National Security Authority
The Secretary for T3P/1
PO Box 56 56
London EC1A 1AH
United Kingdom
Telephone: (44) 20 72 70 87 51
Fax: (44) 20 76 30 14 28

▼B

Anhang 2

▼M1

Vergleich von Sicherheitseinstufungen

EU Einstufung	Très Secret UE/EU Top Secret	Secret UE	Confidentiel UE	Restreint UE
Belgien	Très Secret Zeer Geheim	Secret Geheim	Confidentiel Vertrouwelijk	Diffusion restreinte Beperkte verspreiding
Tschechische Republik	Přísně tajné	Tajné	Důvěrné	Vyhrazené
Dänemark	Yderst hemmeligt	Hemmeligt	Fortroligt	Til tjenestebrug
Deutschland	Streng geheim	Geheim	VS ([2]) — Vertraulich	VS — Nur für den Dienstgebrauch
Estland	Täiesti salajane	Salajane	Konfidentsiaalne	Piiratud
Griechenland	Άκρως απόρρητο Abk: ΑΑΠ	Απόρρητο Abk: (ΑΠ)	Εμπιστευτικό ΕΕ Abk: (ΕΜ)	Περιορισμένης χρήσης Abk: (ΠΧ)
Spanien	Secreto	Reservado	Confidencial	Difusión limitada
Frankreich	Très Secret Défense ([1])	Secret Défense	Confidentiel Défense	Diffusion restreinte
Irland	Top Secret	Secret	Confidential	Restricted
Italien	Segretissimo	Segreto	Riservatissimo	Riservato
Zypern	Άκρως απόρρητο	Απόρρητο	Εμπιστευτικό ΕΕ	Περιορισμένης χρήσης
Lettland	Sevišķi slepeni	Slepeni	Konfidenciāli	Dienesta vajadzībām
Litauen	Visiškai slaptai	Slaptai	Konfidencialiai	Riboto naudojimo
Luxemburg	Très Secret	Secret	Confidentiel	Diffusion restreinte
Ungarn	Szigorúan titkos!	Titkos!	Bizalmas!	Korlátozott terjesztésű!
Malta	L-Ogħla Segretezza	Sigriet	Kunfidenzjali	Ristrett

▼M1

EU Einstufung	Très Secret UE/EU Top Secret	Secret UE	Confidentiel UE	Restreint UE
Niederlande	STG Zeer Geheim	STG Geheim	STG Confidentieel	—
Österreich	Streng geheim	Geheim	Vertraulich	Eingeschränkt
Polen	Ściśle tajne	Tajne	Poufne	Zastrzeżone
Portugal	Muito Secreto	Secreto	Confidencial	Reservado
Slowenien	Strogo tajno	Tajno	Zaupno	SVN Interno
Slowakei	Prísne tajné	Tajné	Dôverné	Vyhradené
Finnland	Erittäin salainen	Erittäin salainen	Salainen	Luottamuksellinen
Schweden	Kvalificerat hemlig	Hemlig	Hemlig	Hemlig
Vereinigtes Königreich	Top Secret	Secret	Confidential	Restricted
NATO Einstufung	Cosmic Top Secret	NATO Secret	NATO Confidential	NATO Restricted
WEU Einstufung	Focal Top Secret	WEU Secret	WEU Confidential	WEU Restricted

([1]) Frankreich: die Einstufung „Très Secret Défense“, die für Regierungsorganisationen gilt, darf nur mit Zustimmung des Premierministers geändert werden.
([2]) Deutschland: VS = Verschlusssache

Anhang 3

Leitfaden für die Einstufungspraxis

Dieser Leitfaden hat lediglich Hinweischarakter und darf nicht im Sinne einer Änderung der Kernvorschriften der Abschnitte II und III ausgelegt werden.

Einstufung	Wann	Wer	Kennzeichnung	Herabstufung/Aufhebung des Geheimhaltungsgrades/Vernichtung	
				wer	wann
„TRÈS SECRET UE/EU TOP SECRET“ (STRENG GEHEIM) Diese Einstufung ist nur bei Informationen und Materialien vorzunehmen, deren unbefugte Weitergabe den wesentlichen Interessen der Europäischen Union oder eines oder mehrerer ihrer Mitgliedstaaten außerordentlich schweren Schaden zufügen würde [Abschnitt II § 1].	Eine Kenntnisnahme durch Unbefugte würde bei Gegenständen mit der Kennzeichnung „TRÈS SECRET UE/EU TOP SECRET“ wahrscheinlich Folgendes bewirken: — unmittelbare Gefährdung der inneren Stabilität der EU oder eines ihrer Mitgliedstaaten oder befreundeter Länder, — außerordentlich schwerwiegende Schädigung der Beziehungen zu befreundeten Regierungen, — unmittelbarer Verlust zahlreicher Menschenleben, — außerordentlich schwerwiegende Schädigung der Einsatzfähigkeit oder der Sicherheit von Streitkräften der Mitgliedstaaten oder anderer Partner bzw. der andauernden Wirksamkeit äußerst wertvoller Sicherheits- oder Intelligence-Operationen, — schwere und langfristige Schädigung der Wirtschaft der EU oder ihrer	Mitgliedstaaten: förmlich dazu befugte Personen (Urheber) [Abschnitt III § 4]; Generalsekretariat des Rates: förmlich dazu befugte Personen (Urheber) [Abschnitt III § 4] und GS/HV. Die Urheber bestimmen ein Datum oder einen Zeitraum, nach dessen Ablauf Inhalte herabgestuft oder deren Geheimhaltungsgrade aufgehoben werden können. Andernfalls überprüfen sie spätestens alle fünf Jahre die betreffenden Dokumente, um sicherzustellen, dass die ursprüngliche Einstufung weiterhin erforderlich ist [Abschnitt III § 10].	Die Angabe des Geheimhaltungsgrades „TRÈS SECRET UE/EU TOP SECRET“ ist auf Dokumenten dieser Kategorie, gegebenenfalls mit dem Zusatz „-ESDP“ (ESVP) bei Verteidigungssachen, mit mechanischen Mitteln oder von Hand anzubringen [Abschnitt II § 8]. Die EU-Einstufungen müssen am oberen und am unteren Rand in der Mitte jeder Seite erscheinen, und jede Seite ist zu nummerieren. Jedes Dokument trägt ein Aktenzeichen und ein Datum; das Aktenzeichen wird auf jeder Seite angegeben. Soll eine Verteilung in mehreren Kopien erfolgen, so ist jede Kopie mit einer laufenden Nummer zu versehen, die auf der ersten Seite zusammen mit der Gesamtseitenzahl angegeben wird. Alle Anhänge und Beilagen sind auf der ersten Seite aufzuführen [Abschnitt VII § 1].	Eine Aufhebung des Geheimhaltungsgrades oder Herabstufung erfolgt ausschließlich durch die Urheber oder den GS/HV; die betreffende Stelle unterrichtet alle nachgeordneten Empfänger, denen sie das Original oder eine Kopie des Dokuments zugeleitet hat, über die Änderung [Abschnitt III § 9]. „TRÈS SECRET UE/EU TOP SECRET“-Dokumente werden durch die Zentralregistratur oder die für diese Dokumente zuständige Unterregistratur vernichtet. Jedes der Vernichtung zugeführte Dokument ist in einer Vernichtungsbescheinigung aufzuführen, die von dem für die Überwachung der „TRÈS SECRET UE/EU TOP SECRET“-Dokumente zuständigen Beamten und dem der Vernichtung als Zeuge beiwohnenden Beamten, der einer Sicherheitsüberprüfung für „TRÈS SECRET UE/EU TOP SECRET“-Dokumente unterzogen wurde, zu unterzeichnen ist. Der Vorgang ist im Dienstbuch festzuhalten.	Überzählige Exemplare und nicht länger benötigte Dokumente sind zu vernichten [Abschnitt VII § 31]. „TRÈS SECRET UE/EU TOP SECRET“-Dokumente einschließlich des bei ihrer Herstellung angefallenen und als Verschlusssache einzustufenden Zwischenmaterials, wie fehlerhafte Kopien, Arbeitsentwürfe, maschinenschriftliche Aufzeichnungen und Kohlepapier, sind unter der Aufsicht eines „TRÈS SECRET UE/EU TOP SECRET“-ermächtigten Beamten durch Verbrennen, Einstampfen, Zerkleinern oder andere geeignete Verfahren so zu vernichten, dass der Inhalt weder erkennbar ist noch erkennbar gemacht werden kann [Abschnitt VII § 31].

Einstufung	Wann	Wer	Kennzeichnung	Herabstufung/Aufhebung des Geheimhaltungsgrades/Vernichtung	
				wer	wann
	Mitgliedstaaten.			Die Vernichtungsbescheinigungen sind zusammen mit dem Verteilungsnachweis durch die Registratur zehn Jahre lang aufzubewahren [Abschnitt VII § 31].	
„SECRET UE“ (GEHEIM) Diese Einstufung ist nur bei Informationen und Materialien vorzunehmen, deren unbefugte Weitergabe den wesentlichen Interessen der Europäischen Union oder eines oder mehrerer ihrer Mitgliedstaaten schweren Schaden zufügen würde [Abschnitt II § 2].	Eine Kenntnisnahme durch Unbefugte würde bei Gegenständen mit der Kennzeichnung „SECRET UE“ wahrscheinlich Folgendes bewirken: — Hervorrufung internationaler Spannungen, — schwerwiegende Schädigung der Beziehungen zu befreundeten Regierungen, — unmittelbare Bedrohung von Leben oder schwerwiegende Beeinträchtigung der öffentlichen Ordnung oder der individuellen Sicherheit oder Freiheit, — schwerwiegende Schädigung der Einsatzfähigkeit oder der Sicherheit von Streitkräften der Mitgliedstaaten oder anderer Partner bzw. der andauernden Wirksamkeit sehr wertvoller Sicherheits- oder Intelligence-Operationen, — erhebliche materielle Schädigung der finanziellen, monetären, wirtschaftlichen und handelspolitischen Inter-	Mitgliedstaaten: befugte Personen (Urheber) [Abschnitt III § 2]; Generalsekretariat des Rates und dezentrale EU-Einrichtungen: befugte Personen (Urheber) [Abschnitt III § 2], Generaldirektoren und GS/HV. Die Urheber bestimmen ein Datum oder einen Zeitraum, nach dessen Ablauf Inhalte herabgestuft oder deren Geheimhaltungsgrade aufgehoben werden können. Andernfalls überprüfen sie spätestens alle fünf Jahre die betreffenden Dokumente, um sicherzustellen, dass die ursprüngliche Einstufung weiterhin erforderlich ist [Abschnitt III § 1].	Die Angabe des Geheimhaltungsgrades „SECRET UE“ ist auf Dokumenten dieser Kategorie, gegebenenfalls mit dem Zusatz „-ESDP“ (ESVP) bei Verteidigungssachen, mit mechanischen Mitteln oder von Hand anzubringen [Abschnitt III § 8]. Die EU-Einstufungen müssen am oberen und am unteren Rand in der Mitte jeder Seite erscheinen, und jede Seite ist zu nummerieren. Jedes Dokument trägt ein Aktenzeichen und ein Datum; das Aktenzeichen wird auf jeder Seite angegeben. Soll eine Verteilung in mehreren Kopien erfolgen, so ist jede Kopie mit einer laufenden Nummer zu versehen, die auf der ersten Seite zusammen mit der Gesamtseitenzahl angegeben wird. Alle Anhänge und Beilagen sind auf der ersten Seite aufzuführen [Abschnitt VII § 1].	Eine Aufhebung des Geheimhaltungsgrades oder Herabstufung erfolgt ausschließlich durch die Urheber oder den GS/HV; die betreffende Stelle unterrichtet alle nachgeordneten Empfänger, denen sie das Original oder eine Kopie des Dokuments zugeleitet hat, über die Änderung [Abschnitt VII § 9]. „SECRET UE“-Dokumente werden von der für diese Dokumente zuständigen Registratur unter der Aufsicht einer sicherheitsüberprüften Person vernichtet. „SECRET UE“-Dokumente, die vernichtet werden, sind auf Vernichtungsbescheinigungen aufzuführen, die zu unterzeichnen und zusammen mit dem Verteilungsnachweis durch die Registratur mindestens drei Jahre lang aufzubewahren sind [Abschnitt VII § 32].	Überzählige Exemplare und nicht länger benötigte Dokumente sind zu vernichten [Abschnitt VII § 31]. „SECRET UE“-Dokumente einschließlich des bei ihrer Herstellung angefallenen und als Verschlusssache einzustufenden Zwischenmaterials, wie fehlerhafte Kopien, Arbeitsentwürfe, maschinenschriftliche Aufzeichnungen und Kohlepapier, sind durch Verbrennen, Einstampfen, Zerkleinern oder andere geeignete Verfahren so zu vernichten, dass der Inhalt weder erkennbar ist noch erkennbar gemacht werden kann [Abschnitt VII §§ 31 und 32].

Einstufung	Wann	Wer	Kennzeichnung	Herabstufung/Aufhebung des Geheimhaltungsgrades/Vernichtung	
				wer	wann
	essen der EU oder eines ihrer Mitgliedstaaten.				
„CONFIDENTIEL UE“ (VS — VERTRAULICH/VERTRAULICH) Diese Einstufung ist bei Informationen und Materialien vorzunehmen, deren unbefugte Weitergabe den wesentlichen Interessen der Europäischen Union oder eines oder mehrerer ihrer Mitgliedstaaten abträglich wären [Abschnitt II § 3].	Eine Kenntnisnahme durch Unbefugte würde bei Gegenständen mit der Kennzeichnung „CONFIDENTIEL UE“ wahrscheinlich Folgendes bewirken: — konkrete Schädigung diplomatischer Beziehungen in dem Sinne, dass förmliche Proteste oder andere Sanktionen hervorgerufen werden, — Beeinträchtigung individueller Sicherheit oder Freiheit, — Schädigung der Einsatzfähigkeit oder der Sicherheit von Streitkräften der Mitgliedstaaten oder anderer Partner bzw. der Wirksamkeit wertvoller Sicherheits- oder Intelligence-Operationen, — wesentliche Beeinträchtigung der finanziellen Tragfähigkeit wichtiger Organisationen, — Behinderung der Ermittlungstätigkeit oder Erleichterung des Begehens schwerer Straftaten, — wesentliche Beeinträchtigung der finanziellen, monetären, wirtschaftlichen und handelspolitischen Interessen der EU oder ihrer Mitgliedstaaten, — ernstliche Behinderung	Mitgliedstaaten: befugte Personen (Urheber) [Abschnitt III § 2]; Generalsekretariat des Rates und dezentrale EU-Einrichtungen: befugte Personen (Urheber) [Abschnitt III § 2], Generaldirektoren und GS/HV. Die Urheber bestimmen ein Datum oder einen Zeitraum, nach dessen Ablauf Inhalte herabgestuft oder deren Geheimhaltungsgrade aufgehoben werden können. Andernfalls überprüfen sie spätestens alle fünf Jahre die betreffenden Dokumente, um sicherzustellen, dass die ursprüngliche Einstufung weiterhin erforderlich ist [Abschnitt III § 10].	Die Angabe des Geheimhaltungsgrades „CONFIDENTIEL UE“ ist auf Dokumenten dieser Kategorie, gegebenenfalls mit dem Zusatz „-ESDP“ (ESVP) bei Verteidigungssachen, mit mechanischen Mitteln und von Hand oder durch Ausdrucken auf vorab mit einem Stempelaufdruck versehenem, registriertem Papier anzubringen [Abschnitt II § 8]. Die EU-Einstufungen müssen am oberen und am unteren Rand in der Mitte jeder Seite erscheinen, und jede Seite ist zu nummerieren. Jedes Dokument trägt ein Aktenzeichen und ein Datum. Alle Anhänge und Beilagen sind auf der ersten Seite aufzuführen [Abschnitt VII § 1].	Eine Aufhebung des Geheimhaltungsgrades oder Herabstufung erfolgt ausschließlich durch die Urheber oder den GS/HV; die betreffende Stelle unterrichtet alle nachgeordneten Empfänger, denen sie das Original oder eine Kopie des Dokuments zugeleitet hat, über die Änderung [Abschnitt VII § 31]. „CONFIDENTIEL UE“-Dokumente werden von der für diese Dokumente zuständigen Registratur unter der Aufsicht einer sicherheitsüberprüften Person vernichtet. Die Vernichtung der Dokumente ist gemäß den einzelstaatlichen Vorschriften bzw., im Falle des Generalsekretariats des Rates oder der dezentralen EU-Einrichtungen, gemäß den Anweisungen des GS/HV zu dokumentieren [Abschnitt VII § 33].	Überzählige Exemplare und nicht länger benötigte Dokumente sind zu vernichten [Abschnitt VII § 31]. „CONFIDENTIEL UE“-Dokumente einschließlich des bei ihrer Herstellung angefallenen und als Verschlusssache einzustufenden Zwischenmaterials, wie fehlerhafte Kopien, Arbeitsentwürfe, maschinenschriftliche Aufzeichnungen und Kohlepapier, sind durch Verbrennen, Einstampfen, Zerkleinern oder andere geeignete Verfahren so zu vernichten, dass der Inhalt weder erkennbar ist noch erkennbar gemacht werden kann [Abschnitt VII §§ 31 und 33].

Einstufung	Wann	Wer	Kennzeichnung	Herabstufung/Aufhebung des Geheimhaltungsgrades/Vernichtung	
				wer	wann
	der Ausarbeitung oder Durchführung wichtiger EU-Politiken, — Abbruch oder erhebliche Unterbrechung wichtiger EU-Aktivitäten.				
„RESTREINT UE“ (VS — NUR FÜR DEN DIENSTGEBRAUCH/ EINGESCHRÄNKT) Diese Einstufung ist bei Informationen und Materialien vorzunehmen, deren unbefugte Weitergabe sich auf die Interessen der Europäischen Union oder eines oder mehrerer ihrer Mitgliedstaaten nachteilig auswirken könnte [Abschnitt II § 4].	Eine Kenntnisnahme durch Unbefugte würde bei Gegenständen mit der Kennzeichnung „RESTREINT UE“ wahrscheinlich Folgendes bewirken: — Belastung diplomatischer Beziehungen, — erhebliche Unannehmlichkeiten für Einzelpersonen, — Erschwerung der Wahrung der Einsatzfähigkeit oder der Sicherheit von Streitkräften der Mitgliedstaaten oder anderer Partner, — finanzielle Verluste oder die Ermöglichung ungerechtfertigter Gewinne oder Vorteile für Einzelpersonen oder Unternehmen, — Bruch eigener Verpflichtungen zur Wahrung der Vertraulichkeit von Informationen, die von dritter Seite erteilt wurden, — Verstoß gegen gesetzlich begründete Einschränkungen der Weitergabe von Informationen, — Beeinträchtigung der Ermittlungstätigkeit oder	Mitgliedstaaten: befugte Personen (Urheber) [Abschnitt III § 2]; Generalsekretariat des Rates und dezentrale EU-Einrichtungen: befugte Personen (Urheber) [Abschnitt III § 2], Generaldirektoren und GS/HV. Die Urheber bestimmen ein Datum oder einen Zeitraum, nach dessen Ablauf Inhalte herabgestuft oder deren Geheimhaltungsgrade aufgehoben werden können. Andernfalls überprüfen sie spätestens alle fünf Jahre die betreffenden Dokumente, um sicherzustellen, dass die ursprüngliche Einstufung weiterhin erforderlich ist [Abschnitt III § 10].	Die Angabe des Geheimhaltungsgrades „RESTREINT UE“ ist auf Dokumenten dieser Kategorie, gegebenenfalls mit dem Zusatz „-ESDP“ (ESVP) bei Verteidigungssachen, mit mechanischen oder elektronischen Mitteln anzubringen [Abschnitt II § 8]. Die EU-Einstufungen müssen am oberen und am unteren Rand in der Mitte jeder Seite erscheinen, und jede Seite ist zu nummerieren. Jedes Dokument trägt ein Aktenzeichen und ein Datum [Abschnitt VII § 1].	Eine Aufhebung des Geheimhaltungsgrades oder Herabstufung erfolgt ausschließlich durch die Urheber oder den GS/HV; die betreffende Stelle unterrichtet alle nachgeordneten Empfänger, denen sie das Original oder eine Kopie des Dokuments zugeleitet hat, über die Änderung [Abschnitt III § 9]. „RESTREINT UE“-Dokumente werden von der für diese Dokumente zuständigen Registratur gemäß den einzelstaatlichen Vorschriften bzw., im Falle des Generalsekretariats des Rates oder der dezentralen EU-Einrichtungen, gemäß den Anweisungen des GS/HV vernichtet [Abschnitt VII § 34].	Überzählige Exemplare und nicht länger benötigte Dokumente sind zu vernichten [Abschnitt VII § 31].

▼B

Einstufung	Wann	Wer	Kennzeichnung	Herabstufung/Aufhebung des Geheimhaltungsgrades/Vernichtung	
				wer	wann
	Erleichterung des Begehens schwerer Straftaten, — Benachteiligung der EU oder ihrer Mitgliedstaaten bei Verhandlungen mit Dritten über handelspolitische oder allgemein politische Fragen, — Behinderung der wirksamen Ausarbeitung oder Durchführung von EU-Politiken, — Gefährdung einer sachgerechten Verwaltung der EU und ihrer Tätigkeiten.				

▼B

Anhang 4

Leitlinien für die Weitergabe von EU-Verschlusssachen an Drittstaaten oder internationale Organisationen

Kooperationsstufe 1

VERFAHREN

1. Für die Weitergabe von EU-Verschlusssachen an Länder, die nicht Unterzeichner des Vertrags über die Europäische Union sind, oder an andere internationale Organisationen, deren Sicherheitskonzept und -vorschriften mit denen der EU vergleichbar sind, ist der Rat zuständig.

2. Der Rat kann seine Entscheidungsbefugnis hinsichtlich der Weitergabe von Verschlusssachen übertragen. Bei seiner Übertragung legt er die Art der Informationen, die weitergegeben werden können, und deren Geheimhaltungsgrad — in der Regel nicht höher als „CONFIDENTIEL UE“ — fest.

3. Vorbehaltlich des Abschlusses eines Geheimschutzabkommens sind die Anträge auf Weitergabe von EU-Verschlusssachen durch die Sicherheitsbehörden der betreffenden Länder oder internationalen Organisationen an den Generalsekretär/Hohen Vertreter zu richten; sie führen Nutzungszweck und Art der Verschlusssache an, die weitergegeben werden soll.

   Anträge können auch durch einen Mitgliedstaat oder eine dezentrale EU-Einrichtung gestellt werden, der bzw. die eine Weitergabe der EU-Verschlusssache für wünschenswert hält; sie führen Ziele und Vorteile einer solchen Weitergabe für die EU sowie Art und Geheimhaltungsgrad der Informationen an, die weitergegeben werden sollen.

4. Der Antrag wird vom Generalsekretariat des Rates geprüft. Dieses
   — holt die Stellungnahme des Mitgliedstaats oder gegebenenfalls der dezentralen EU-Einrichtung ein, von dem bzw. der die Informationen stammen, welche weitergegeben werden sollen;
   — knüpft die nötigen Kontakte zu den Sicherheitsbehörden der als Empfänger vorgesehenen Länder oder internationalen Organisationen, um zu prüfen, ob deren Sicherheitskonzept und -vorschriften gewährleisten können, dass die weitergegebenen Verschlusssachen gemäß diesen Sicherheitsvorschriften geschützt werden;
   — fordert technische Gutachten der nationalen Sicherheitsbehörden der Mitgliedstaaten hinsichtlich der Vertrauenswürdigkeit der als Empfänger vorgesehenen Länder oder internationalen Stellen an.

5. Das Generalsekretariat des Rates legt dem Rat den Antrag und die Empfehlung des Sicherheitsbüros zur Entscheidung vor.

VON DEN EMPFÄNGERN EINZUHALTENDE SICHERHEITSVORSCHRIFTEN

6. Der Generalsekretär/Hohe Vertreter stellt den als Empfänger vorgesehenen Ländern oder internationalen Organisationen den Beschluss des Rates zur Genehmigung der Weitergabe von EU-Verschlusssachen zu und übermittelt ihnen die für notwendig erachtete Anzahl von Exemplaren dieser Sicherheitsvorschriften. Wurde der Antrag von einem Mitgliedstaat gestellt, so teilt dieser Staat dem Empfänger die Genehmigung der Weitergabe mit.

   Der Weitergabebeschluss tritt nur dann in Kraft, wenn die Empfänger sich schriftlich verpflichten,
   — die Informationen nur zu den vereinbarten Zwecken zu nutzen;
   — die Informationen gemäß diesen Sicherheitsvorschriften und insbesondere unter Einhaltung der nachfolgenden speziellen Bestimmungen zu schützen.

7. *Personal*

   a) Die Zahl der Bediensteten, die Zugang zu EU-Verschlusssachen erhalten, beschränkt sich nach dem Grundsatz „Kenntnis nur wenn nötig“ strikt auf die Personen, deren Aufgabenstellung diesen Zugang erfordert.

   b) Alle Bediensteten oder Staatsangehörigen, denen der Zugang zu Informationen des Geheimhaltungsgrades „CONFIDENTIEL UE“ oder darüber gestattet wird, müssen Inhaber einer für die betreffende Stufe gültigen Sicherheitsunbedenklichkeitsbescheinigung oder einer entsprechenden Sicherheitsermächtigung sein, wobei diese Sicherheitsunbedenklichkeitsbescheinigung oder die Ermächtigung von der Regierung ihres eigenen Staates ausgestellt beziehungsweise erteilt wird.

▼B

8. *Übermittlung von Dokumenten*

   a) Die praktischen Verfahren für die Übermittlung von Dokumenten werden durch ein Abkommen nach Maßgabe der Bestimmungen des Abschnitts VII dieser Sicherheitsvorschriften festgelegt. Darin wird insbesondere die Registratur angeführt, an die EU-Verschlusssachen weitergegeben werden sollen.

   b) Umfassen die Verschlusssachen, deren Weitergabe vom Rat genehmigt wird, Informationen der Stufe „TRÈS SECRET UE/EU TOP SECRET", so richtet der Empfänger ein EU-Zentralregister und gegebenenfalls EU-Unterregister ein. Für diese Register gelten die Bestimmungen des Abschnitts VIII dieser Sicherheitsvorschriften.

9. *Registrierung*

   Sobald eine Registratur ein als „CONFIDENTIEL UE" oder höher eingestuftes EU-Dokument erhält, trägt sie dieses Dokument in einem eigens dafür angelegten Register ihrer Organisation ein; dieses Register umfasst Spalten, in denen das Eingangsdatum, die Bestimmungsmerkmale des Dokuments (Datum, Aktenzeichen und Nummer des Exemplars), seinen Geheimhaltungsgrad, sein Titel, der Name oder Titel des Empfängers, das Rücksendedatum der Empfangsbestätigung und das Datum, zu dem das Dokument an den EU-Herausgeber zurückgesandt oder vernichtet wird, zu verzeichnen sind.

10. *Vernichtung*

   a) EU-Verschlusssachen sind gemäß den Anweisungen des Abschnitts VI dieser Sicherheitsvorschriften zu vernichten. Bei Dokumenten der Stufen „SECRET UE" und „TRÈS SECRET UE/EU TOP SECRET" sind Kopien der Vernichtungsbescheinigungen an die EU-Registratur zu senden, von der die Dokumente übermittelt wurden.

   b) EU-Verschlusssachen sind in die Notfall-Vernichtungspläne einzubeziehen, die die zuständigen Stellen des Empfängers für ihre eigenen Verschlusssachen aufgestellt haben.

11. *Schutz der Dokumente*

   Es sind alle erforderlichen Maßnahmen zu ergreifen, damit Unbefugte keinen Zugang zu EU-Verschlusssachen erhalten.

12. *Kopien, Übersetzungen und Auszüge*

   Fotokopien, Übersetzungen oder Auszüge eines als „CONFIDENTIEL UE" oder „SECRET UE" eingestuften Dokuments dürfen nur mit Genehmigung des Leiters des betroffenen Sicherheitsorgans angefertigt werden, der diese Kopien, Übersetzungen oder Auszüge registriert und prüft und nötigenfalls mit einem Stempel versieht.

   Die Vervielfältigung oder Übersetzung eines Dokuments der Stufe „TRÈS SECRET UE/EU TOP SECRET" kann nur von der Behörde genehmigt werden, von der das Dokument stammt; sie legt die Anzahl der zulässigen Exemplare fest; kann die Behörde, von der das Dokument stammt, nicht ermittelt werden, so ist der Antrag an das Sicherheitsbüro des Generalsekretariats des Rates zu richten.

13. *Verstöße gegen die Sicherheitsvorschriften*

   Bei Verstößen gegen die Sicherheitsvorschriften im Zusammenhang mit einer EU-Verschlusssache oder bei einem entsprechenden Verdacht sollten vorbehaltlich des Abschlusses eines Geheimschutzabkommens unverzüglich folgende Schritte unternommen werden:

   a) Einleitung einer Untersuchung zur Klärung der Umstände des Verstoßes gegen die Sicherheitsvorschriften;

   b) Benachrichtigung des Sicherheitsbüros des Generalsekretariats des Rates und der nationalen Sicherheitsbehörde sowie der Behörde, von der die Informationen stammen, oder aber gegebenenfalls eindeutige Mitteilung, dass die letztgenannte Behörde nicht benachrichtigt wurde;

   c) Ergreifen von Maßnahmen, damit die Folgen eines Verstoßes gegen die Sicherheitsvorschriften so weit wie möglich eingeschränkt werden;

   d) erneute Prüfung und Durchführung von Maßnahmen, damit sich der Vorfall nicht wiederholt;

   e) Durchführung der vom Sicherheitsbüro des Generalsekretariats des Rates empfohlenen Maßnahmen, damit sich der Vorfall nicht wiederholt.

14. *Inspektionen*

   Das Sicherheitsbüro des Generalsekretariats des Rates kann im Benehmen mit den betreffenden Staaten oder internationalen Organisationen eine

▼B

Bewertung der Effizienz der Maßnahmen zum Schutz der weitergegebenen EU-Verschlusssachen vornehmen.

15. *Berichterstattung*

Solange Staaten oder internationale Organisationen EU-Verschlusssachen aufbewahren, erstellen sie vorbehaltlich des Abschlusses eines Geheimschutzabkommens jährlich zu dem Datum, das in der Genehmigung zur Informationsweitergabe angegeben ist, einen Bericht, mit dem bestätigt wird, dass diese Sicherheitsvorschriften eingehalten wurden.

▼B

Anhang 5

Leitlinien für die Weitergabe von EU-Verschlusssachen an Drittstaaten oder internationale Organisationen

Kooperationsstufe 2

VERFAHREN

1. Für die Weitergabe von EU-Verschlusssachen an Drittstaaten oder internationale Organisationen, deren Sicherheitskonzept und -vorschriften deutlich von denen der EU abweichen, ist der Rat zuständig. Prinzipiell beschränkt sich die Weitergabe auf Informationen bis einschließlich des Geheimhaltungsgrades „SECRET UE“; einzelstaatliche Informationen, die speziell den Mitgliedstaaten vorbehalten sind, und durch besondere Kennzeichnungen geschützte Kategorien von EU-Verschlusssachen sind davon ausgeschlossen.

2. Der Rat kann seine Entscheidungsbefugnis in diesem Bereich übertragen. Bei einer Übertragung legt er in den Grenzen der in Nummer 1 festgelegten Einschränkungen die Art der Informationen, die weitergegeben werden können, und deren Geheimhaltungsgrad — nicht höher als „RESTREINT UE“ — fest.

3. Vorbehaltlich des Abschlusses eines Geheimschutzabkommens sind die Anträge auf Weitergabe von EU-Verschlusssachen durch die Sicherheitsbehörden der betreffenden Länder oder internationalen Organisationen an den Generalsekretär/Hohen Vertreter zu richten; sie führen Nutzungszweck, Art und Geheimhaltungsgrad der Informationen an, die weitergegeben werden sollen.

   Anträge können auch durch einen Mitgliedstaat oder eine dezentrale EU-Einrichtung gestellt werden, der bzw. die eine Weitergabe der EU-Verschlusssache für wünschenswert hält; sie führen Ziele und Vorteile einer solchen Weitergabe für die EU sowie Art und Geheimhaltungsgrad der Informationen an, die weitergegeben werden sollen.

4. Der Antrag wird vom Generalsekretariat des Rates geprüft. Dieses

   — holt die Stellungnahme des Mitgliedstaats oder gegebenenfalls der dezentralen EU-Einrichtung ein, von dem bzw. der die Informationen stammen, welche weitergegeben werden sollen;

   — knüpft erste Kontakte zu den Sicherheitsbehörden der als Empfänger vorgesehenen Länder oder internationalen Organisation, um Informationen über deren Sicherheitskonzept und -vorschriften einzuholen, und insbesondere eine Vergleichstabelle der in der EU und in den betreffenden Staaten oder Organisationen geltenden Geheimhaltungsgrade zu erstellen;

   — beruft eine Sitzung des Sicherheitsausschusses des Rates ein oder ersucht, falls erforderlich im Wege des vereinfachten schriftlichen Verfahrens, die nationalen Sicherheitsbehörden der Mitgliedstaaten um Prüfung im Hinblick auf ein technisches Gutachten des Sicherheitsausschusses.

5. In seinem technischen Gutachten äußert sich der Sicherheitsausschuss des Rates zu folgenden Aspekten:

   — Vertrauenswürdigkeit der als Empfänger vorgesehenen Staaten oder internationalen Organisationen im Hinblick auf eine Bewertung der für die EU oder deren Mitgliedstaaten bestehenden Sicherheitsrisiken;

   — Bewertung der Fähigkeit des Empfängers, von der EU weitergegebene Verschlusssachen zu schützen;

   — Vorschläge für die praktische Behandlung der EU-Verschlusssachen (beispielsweise Übermittlung bearbeiteter Textfassungen) und der übermittelten Dokumente (Beibehaltung oder Streichung von EU-Einstufungsvermerken, besonderen Kennzeichnungen usw.);

   — Herabstufung oder Aufhebung des Geheimhaltungsgrades durch die herausgebende Stelle, bevor die Informationen an die als Empfänger vorgesehenen Länder oder internationalen Organisationen weitergegeben werden ([1]).

6. Der Generalsekretär/Hohe Vertreter legt dem Rat den Antrag sowie das vom Sicherheitsbüro des Generalsekretariats des Rates eingeholte technische Gutachten des Sicherheitsausschusses zur Entscheidung vor.

([1]) Dies hat zur Folge, dass die herausgebende Stelle das Verfahren des Abschnitts III Nummer 9 für alle in der EU im Umlauf befindlichen Exemplare anzuwenden hat.

▼B

VON DEN EMPFÄNGERN EINZUHALTENDE SICHERHEITSVORSCHRIFTEN

7. Der Beschluss des Rates zur Genehmigung der Weitergabe von EU-Verschlusssachen wird den als Empfänger vorgesehenen Ländern oder internationalen Organisationen vom Generalsekretär/Hohen Vertreter zusammen mit einer Vergleichstabelle der in der EU und in den betreffenden Staaten bzw. Organisationen geltenden Geheimhaltungsgrade bekannt gemacht. Wurde der Antrag von einem Mitgliedstaat gestellt, so teilt dieser Staat dem Empfänger die Genehmigung der Weitergabe mit.

   Der Weitergabebeschluss tritt nur dann in Kraft, wenn die Empfänger sich schriftlich verpflichten,

   — die Informationen nur zu den vereinbarten Zwecken zu nutzen;

   — die Informationen gemäß den Sicherheitsvorschriften des Rates zu schützen.

8. Es werden folgende Schutzvorschriften festgelegt, sofern nicht der Rat nach Einholung des technischen Gutachtens des Sicherheitsausschusses des Rates ein besonderes Verfahren (Streichung des Einstufungsvermerks, der besonderen Kennzeichnung usw.) für die Behandlung von EU-Verschlusssachen vorsieht.

   Die Vorschriften werden in diesem Fall angepasst.

9. *Personal*

   a) Die Zahl der Bediensteten, die Zugang zu EU-Verschlusssachen erhalten, muss sich nach dem Grundsatz „Kenntnis nur wenn nötig“ strikt auf die Personen beschränken, deren Aufgabenstellung diesen Zugang erfordert.

   b) Alle Bediensteten oder Staatsangehörigen, denen der Zugang zu von der EU weitergegebenen Verschlusssachen gestattet wird, müssen Inhaber einer nationalen Sicherheitsunbedenklichkeitsbescheinigung oder einer Zugangsermächtigung für den Fall nationaler Verschlusssachen, auf einer entsprechenden und der EU-Einstufung gemäß der Vergleichstabelle gleichwertigen Stufe sein.

   c) Diese nationalen Sicherheitsunbedenklichkeitsbescheinigungen oder Zugangsermächtigungen werden dem Generalsekretär/Hohen Vertreter zur Information mitgeteilt.

10. *Übermittlung von Dokumenten*

   a) Die praktischen Verfahren für die Übermittlung von Dokumenten werden vom Sicherheitsbüro des Generalsekretariats des Rates und den Sicherheitsbehörden der alsEmpfänger vorgesehenen Staaten oder internationalen Organisationen auf der Grundlage der Vorschriften des Abschnitts VII vereinbart. Sie regeln insbesondere die genaue Anschrift, an die die Dokumente zuzustellen sind, sowie den Kurier oder Postdienst, der für die Übermittlung von EU-Verschlusssachen eingesetzt wird.

   b) Verschlusssachen des Geheimhaltungsgrades „CONFIDENTIEL UE“ und darüber werden in doppeltem Umschlag zugestellt. Der innere Umschlag wird mit „EU“ und dem Geheimhaltungsgrad gekennzeichnet. Für jede Verschlusssache wird eine Empfangsbescheinigung beigelegt. In der Empfangsbescheinigung, die als solche nicht eingestuft ist, werden nur die Bestimmungsmerkmale des Dokuments (sein Aktenzeichen, das Datum, die Nummer des Exemplars) und dessen Sprachfassung, nicht aber der Titel aufgeführt.

   c) Der innere Umschlag wird in den äußeren Umschlag geschoben, der zu Empfangszwecken eine Paketnummer trägt. Auf dem äußeren Umschlag wird kein Geheimhaltungsgrad angegeben.

   d) Den Kurieren wird stets eine Empfangsbescheinigung mit der Paketnummer ausgehändigt.

11. *Registrierung am Bestimmungsort*

   Die nationale Sicherheitsbehörde des Empfängerstaats, die ihr gleichzusetzende Stelle, die in diesem Staat im Auftrag ihrer Regierung die von der EU weitergegebene Verschlusssache in Empfang nimmt, oder das Sicherheitsbüro der als Empfänger vorgesehenen internationalen Organisation legt ein spezielles Register für EU-Verschlusssachen an und registriert diese, sobald sie dort eingehen. Dieses Register umfasst Spalten, in denen das Eingangsdatum, die Bestimmungsmerkmale des Dokuments (Datum, Aktenzeichen und Nummer des Exemplars), sein Geheimhaltungsgrad, sein Titel, der Name oder Titel des Empfängers, das Rücksendedatum der Empfangsbescheinigung und das Datum, zu dem das Dokument an die EU zurückgesandt oder vernichtet wird, zu verzeichnen sind.

▼B

12. *Rücksendung von Dokumenten*

Bei Rücksendung einer Verschlusssache durch den Empfänger an den Rat oder an den Mitgliedstaat, der die Verschlusssache weitergegeben hat, ist das Verfahren der Nummer 10 zu befolgen.

13. *Schutz der Dokumente*

a) Nicht benutzte Dokumente sind in einem Sicherheitsbehältnis aufzubewahren, das für die Aufbewahrung nationaler Verschlusssachen desselben Geheimhaltungsgrades zugelassen ist. Das Behältnis darf keine Angaben tragen, die Aufschluss über seinen Inhalt geben könnten; dieser Inhalt ist nur den Personen zugänglich, die zur Behandlung von EU-Verschlusssachen ermächtigt sind. Wenn Kombinationsschlösser verwendet werden, so darf die Kombination nur den Bediensteten des Staates oder der Organisation bekannt sein, denen der Zugang zu der in dem Behältnis aufbewahrten EU-Verschlusssache gestattet ist; die Kombination ist alle sechs Monate oder — bei Versetzung eines Bediensteten, bei Entzug der Sicherheitsermächtigung für einen der Bediensteten, denen die Kombination bekannt ist, oder bei Gefahr der Verletzung des Kombinationsgeheimnisses — früher zu ändern.

b) EU-Verschlusssachen dürfen aus dem Sicherheitsbehältnis nur von Bediensteten entnommen werden, die aufgrund einer Sicherheitsüberprüfung zum Zugang zu EU-Verschlusssachen ermächtigt sind und eine Kenntnisnahme benötigen. Solange die Dokumente in ihrem Besitz sind, tragen die Bediensteten die Verantwortung für deren sichere Aufbewahrung und insbesondere dafür, dass Unbefugte keinen Zugang zu den Dokumenten erhalten. Sie sorgen außerdem dafür, dass die Dokumente nach erfolgter Einsichtnahme sowie außerhalb der Arbeitszeiten in einem Sicherheitsbehältnis aufbewahrt werden.

c) Fotokopien von bzw. Auszüge aus als „CONFIDENTIEL UE“ oder darüber eingestuften Dokumenten dürfen nur mit Genehmigung des Sicherheitsbüros des Generalsekretariats des Rates angefertigt werden.

d) Das Verfahren zur raschen und vollständigen Vernichtung der Dokumente im Notfall sollte im Benehmen mit dem Sicherheitsbüro des Generalsekretariats des Rates festgelegt und bestätigt werden.

14. *Physische Sicherheit*

a) Nicht benutzte Sicherheitsbehältnisse, die zur Aufbewahrung von EU-Verschlusssachen dienen, sind stets verschlossen zu halten.

b) Wartungs- oder Reinigungspersonal, das einen Raum betritt, in dem solche Sicherheitsbehältnisse untergebracht sind, oder dort arbeitet, muss stets von einem Angehörigen des Sicherheitsdienstes des Staates oder der Organisation oder von dem Bediensteten begleitet werden, der speziell für die Sicherheitsaufsicht über diesen Raum verantwortlich ist.

c) Außerhalb der normalen Arbeitszeiten (nachts, an Wochenenden oder Feiertagen) sind die Sicherheitsbehältnisse, die EU-Verschlusssachen enthalten, entweder durch einen Wachbeamten oder durch ein automatisches Alarmsystem zu sichern.

15. *Verstöße gegen die Sicherheitsvorschriften*

Bei Verstößen gegen die Sicherheitsvorschriften im Zusammenhang mit einer EU-Verschlusssache oder bei einem entsprechenden Verdacht, sollten unverzüglich folgende Schritte unternommen werden:

a) sofortige Übermittlung eines Berichts an das Sicherheitsbüro des Generalsekretariats des Rates oder an die nationale Sicherheitsbehörde des Mitgliedstaats, der die Initiative zur Übermittlung von Dokumenten ergriffen hat (mit einer Abschrift an das Sicherheitsbüro des Generalsekretariats des Rates);

b) Einleitung einer Untersuchung und nach deren Abschluss Übermittlung eines umfassenden Berichts an die Sicherheitsstelle (siehe Buchstabe a)). Anschließend sollten die nötigen Maßnahmen ergriffen werden, um Abhilfe zu schaffen.

16. *Inspektionen*

Das Sicherheitsbüro des Generalsekretariats des Rates kann im Benehmen mit den betreffenden Staaten oder internationalen Organisationen eine Bewertung der Effizienz der Maßnahmen zum Schutz der weitergegebenen EU-Verschlusssachen vornehmen.

▼B

17. *Berichterstattung*

Solange Staaten oder Organisationen EU-Verschlusssachen aufbewahren, erstellen sie jährlich zu dem Datum, das in der Genehmigung zur Informationsweitergabe angegeben ist, einen Bericht, mit dem bestätigt wird, dass diese Sicherheitsvorschriften eingehalten wurden.

▼B

Anhang 6

Leitlinien für die Weitergabe von EU-Verschlusssachen an Drittstaaten oder internationale Organisationen

Kooperationsstufe 3

VERFAHREN

1. Es kann gelegentlich vorkommen, dass der Rat unter bestimmten Umständen mit Staaten oder Organisationen zusammenarbeiten möchte, die die von diesen Sicherheitsvorschriften verlangten Garantien nicht bieten können; eine solche Zusammenarbeit kann jedoch die Weitergabe von EU-Verschlusssachen erforderlich machen. Speziell den Mitgliedstaaten vorbehaltene nationale Informationen sind von dieser Weitergabe ausgenommen.

2. Unter diesen besonderen Umständen werden Kooperationsanträge an die EU, gleichgültig ob sie von Drittstaaten oder internationalen Organisationen oder aber von den Mitgliedstaaten oder gegebenenfalls von dezentralen EU-Einrichtungen ausgehen, vom Rat zunächst inhaltlich geprüft; erforderlichenfalls holt der Rat eine Stellungnahme des Mitgliedstaats oder der dezentralen Einrichtung ein, von dem bzw. der die Informationen stammen. Der Rat prüft die Ratsamkeit einer Weitergabe von Verschlusssachen, bewertet, inwieweit der Empfänger Kenntnis von diesen Informationen haben muss, und beschließt, welche Kategorien von Verschlusssachen übermittelt werden können.

3. Spricht der Rat sich für eine Weitergabe von Informationen aus, so obliegt es dem Generalsekretär/Hohen Vertreter, im Hinblick auf ein technisches Gutachten des Sicherheitsausschusses des Rates eine Sitzung dieses Ausschusses einzuberufen oder, falls zweckmäßig im Wege des vereinfachten schriftlichen Verfahrens, die nationalen Sicherheitsbehörden der Mitgliedstaaten um Auskunft zu ersuchen.

4. In seinem technischen Gutachten äußert sich der Sicherheitsausschuss des Rates zu folgenden Aspekten:

   a) Einschätzung der für die EU oder ihre Mitgliedstaaten bestehenden Sicherheitsrisiken;

   b) Einstufung der Informationen, die weitergegeben werden können, gegebenenfalls hinsichtlich der Art dieser Informationen;

   c) Herabstufung oder Aufhebung des Geheimhaltungsgrades der Informationen durch die herausgebende Stelle, bevor die Informationen an die betreffenden Länder oder internationalen Organisationen weitergegeben werden ([1]);

   d) Behandlung der Dokumente, die weitergegeben werden sollen (siehe Nummer 5);

   e) mögliche Übermittlungswege (mit dem öffentlichen Postdienst, über öffentliche oder sichere Telekommunikationssysteme, mit Diplomatenpost, sicherheitsüberprüften Kurieren, usw.).

5. Dokumente, die an Staaten oder Organisationen weitergegeben werden, die unter diesen Anhang fallen, werden prinzipiell ohne Bezugnahme auf die Quelle oder eine EU-Einstufung erstellt. Der Sicherheitsausschuss des Rates kann empfehlen,

   — eine besondere Kennzeichnung oder einen Codenamen zu verwenden;

   — ein spezielles Einstufungssystem zu verwenden, bei dem die Sensibilität der Informationen im Zusammenhang mit den Kontrollmaßnahmen gesehen wird, die aufgrund der vom Empfänger befolgten Methoden für die Übermittlung von Dokumenten erforderlich werden (siehe Beispiele unter Nummer 14).

6. Das Sicherheitsbüro des Generalsekretariats des Rates unterbreitet dem Rat das technische Gutachten des Sicherheitsausschusses und fügt nötigenfalls Vorschläge für die Kompetenzübertragungen hinzu, die zur Wahrnehmung der Aufgabe, insbesondere bei Dringlichkeit, erforderlich sind.

7. Hat der Rat die Weitergabe von EU-Verschlusssachen beschlossen und die praktischen Durchführungsverfahren festgelegt, knüpft das Sicherheitsbüro des Generalsekretariats des Rates die nötigen Kontakte mit der Sicherheits-

([1]) Dies hat zur Folge, dass die herausgebende Stelle das Verfahren des Abschnitts III Nummer 9 für alle in der EU im Umlauf befindlichen Exemplare anzuwenden hat.

▼B

behörde der betreffenden Staaten oder Organisationen, um die Anwendung der geplanten Sicherheitsmaßnahmen zu erleichtern.

8. Als Referenzunterlage stellt das Sicherheitsbüro des Generalsekretariats des Rates allen Mitgliedstaaten und, soweit zweckmäßig, den betroffenen dezentralen EU-Einrichtungen eine Übersicht zu, in der Art und Einstufung der Informationen sowie die Organisationen und Länder aufgeführt werden, an welche die Informationen gemäß dem Beschluss des Rates weitergegeben werden können.

9. Die nationale Sicherheitsbehörde des Mitgliedstaates, der die Weitergabe vornimmt, oder das Sicherheitsbüro des Generalsekretariats des Rates trifft alle erforderlichen Maßnahmen, um eine Bewertung späteren Schadens und eine Überarbeitung der Verfahren zu erleichtern.

10. Der Rat wird erneut befasst, wenn die Bedingungen für eine Zusammenarbeit sich ändern.

VON DEN EMPFÄNGERN EINZUHALTENDE SICHERHEITSVORSCHRIFTEN

11. Der Beschluss des Rates zur Genehmigung der Weitergabe von EU-Verschlusssachen wird den als Empfänger vorgesehenen Ländern oder internationalen Organisationen vom Generalsekretär/Hohen Vertreter zusammen mit den vom Sicherheitsausschuss des Rates vorgeschlagenen und vom Rat angenommenen Schutzvorschriften bekannt gemacht. Wurde der Antrag von einem Mitgliedstaat gestellt, so teilt dieser Staat dem Empfänger die Genehmigung der Weitergabe mit.

    Der Weitergabebeschluss tritt nur dann in Kraft, wenn die Empfänger sich schriftlich verpflichten,

    — die Informationen nur zum Zweck der vom Rat beschlossenen Zusammenarbeit zu nutzen;

    — den Informationen den vom Rat verlangten Schutz zu gewähren.

12. *Übermittlung von Dokumenten*

    a) Die praktischen Verfahren für die Übermittlung von Dokumenten werden vom Sicherheitsbüro des Generalsekretariats des Rates und den Sicherheitsbehörden der als Empfänger vorgesehenen Staaten oder internationalen Organisationen vereinbart. Sie regeln insbesondere die genaue Anschrift, an die die Dokumente zuzustellen sind.

    b) Verschlusssachen des Geheimhaltungsgrades „CONFIDENTIEL UE“ und darüber werden in doppeltem Umschlag zugestellt. Der innere Umschlag trägt einen eigenen Stempel oder den festgelegten Codenamen und einen Vermerk der für dieses Dokument genehmigten speziellen Einstufung. Für jede Verschlusssache wird eine Empfangsbescheinigung beigelegt. In der Empfangsbescheinigung, die als solche nicht eingestuft ist, werden nur die Bestimmungsmerkmale des Dokuments (sein Aktenzeichen, das Datum, die Nummer des Exemplars) und dessen Sprachfassung, nicht aber der Titel, aufgeführt.

    c) Der innere Umschlag wird in den äußeren Umschlag geschoben, der zu Empfangszwecken eine Paketnummer trägt. Auf dem äußeren Umschlag wird kein Geheimhaltungsgrad angegeben.

    d) Den Kurieren wird stets eine Empfangsbescheinigung mit der Paketnummer ausgehändigt.

13. *Registrierung am Bestimmungsort*

    Die nationale Sicherheitsbehörde des Empfängerstaates, die ihr gleichzusetzende Stelle, die in diesem Staat im Auftrag ihrer Regierung die von der EU weitergegebene Verschlusssache in Empfang nimmt, oder das Sicherheitsbüro der als Empfänger vorgesehenen internationalen Organisation legt ein spezielles Register für EU-Verschlusssachen an und registriert diese, sobald sie dort eingehen. Dieses Register umfasst Spalten, in denen das Eingangsdatum, die Bestimmungsmerkmale des Dokuments (Datum, Aktenzeichen und Nummer des Exemplars), sein Geheimhaltungsgrad, sein Titel, der Name oder Titel des Empfängers, das Rücksendedatum der Empfangsbescheinigung und das Datum, zu dem das Dokument an die EU zurückgesandt oder vernichtet wird, zu verzeichnen sind.

14. *Verwendung und Schutz von ausgetauschten Verschlusssachen*

    a) Der Umgang mit Verschlusssachen des Geheimhaltungsgrades „SECRET UE“ ist auf eigens dafür bestimmte Bedienstete zu beschränken, die über eine Zugangsermächtigung für Informationen dieser Stufe verfügen. Die Informationen werden in Panzerschränken von guter Qualität aufbewahrt, die nur von den Personen geöffnet werden können, die zum Zugang zu den darin befindlichen Informationen berechtigt sind. Die Bereiche, in

▼B

denen diese Panzerschränke untergebracht sind, werden ständig bewacht, und es wird ein Überprüfungssystem eingerichtet, damit sichergestellt ist, dass nur ordnungsmäßig ermächtigten Personen der Zugang gestattet wird. Informationen des Geheimhaltungsgrades „SECRET UE“ werden mit Diplomatenpost, sicheren Postdiensten und sicheren Telekommunikationsmitteln übermittelt. Ein „SECRET UE“-Dokument darf nur mit schriftlicher Genehmigung der herausgebenden Stelle kopiert werden. Alle Kopien werden registriert, und ihre Verteilung wird überwacht. Für alle Verrichtungen mit „SECRET UE“-Dokumenten werden Empfangsbescheinigungen ausgestellt.

b) Der Umgang mit Verschlusssachen des Geheimhaltungsgrades „CONFIDENTIEL UE“ ist auf Bedienstete zu beschränken, die ordnungsgemäß ermächtigt sind, über das Thema informiert zu werden. Die Dokumente werden in verschlossenen Panzerschränken in überwachten Bereichen aufbewahrt.

   Verschlusssachen des Geheimhaltungsgrades „CONFIDENTIEL UE“ werden mit Diplomatenpost, dem militärischen Postdienst und sicheren Telekommunikationsmitteln übermittelt. Die empfangende Stelle kann Kopien anfertigen, deren Anzahl und Verteilung in speziellen Registern zu verzeichnen sind.

c) Der Umgang mit Verschlusssachen des Geheimhaltungsgrades „RESTREINT UE“ ist auf Räume zu beschränken, die Unbefugten nicht zugänglich sind; die Dokumente sind in verschlossenen Behältnissen aufzubewahren. Die Dokumente können mit dem öffentlichen Postdienst als Einschreiben in doppeltem Umschlag und im Zuge von Operationen in Notfällen auch über nicht gesicherte öffentliche Telekommunikationssysteme übermittelt werden. Die Empfänger können Kopien anfertigen.

d) Nicht eingestufte Informationen erfordern keine speziellen Schutzmaßnahmen und können auf dem Postweg und über öffentliche Telekommunikationssysteme übermittelt werden. Die Empfänger können Kopien anfertigen.

15. *Vernichtung*

Dokumente, für die keine Verwendung mehr besteht, sind zu vernichten. Für Verschlusssachen des Geheimhaltungsgrades „RESTREINT UE“ und „CONFIDENTIEL UE“ wird ein entsprechender Vermerk in die speziellen Register aufgenommen. Für „SECRET UE“-Verschlusssachen sind Vernichtungsbescheinigungen auszustellen, die von zwei Personen unterzeichnet werden, die der Vernichtung als Zeuge bewohnen.

16. *Verstöße gegen die Sicherheitsvorschriften*

Wurde bei einer Verschlusssache der Geheimhaltungsgrade „CONFIDENTIEL UE“ oder „SECRET UE“ die Geheimschutzregelung verletzt oder besteht ein entsprechender Verdacht, so leitet die nationale Sicherheitsbehörde des Staates oder der Sicherheitsverantwortliche der Organisation eine Untersuchung der Umstände ein. Bestätigt sich dabei die Verletzung, ist die herausgebende Stelle zu benachrichtigen. Es werden die nötigen Maßnahmen getroffen, um bei ungeeigneten Verfahren oder Aufbewahrungsmethoden, die zu der Verletzung geführt haben, für Abhilfe zu sorgen. Der Generalsekretär/Hohe Vertreter des Rates oder die nationale Sicherheitsbehörde des Mitgliedstaats, die die betreffende Verschlusssache weitergegeben hat, kann den Empfänger um Übermittlung der ausführlichen Untersuchungsergebnisse ersuchen.